Surveillance of Social Media and International Human Rights

Seán Looney

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

École doctorale : EDSJ - Ecole Doctorale Sciences Juridiques
Spécialité : Droits de l'Homme
Unité de recherche : Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes

Surveillance des medias sociaux et Droit international des droits de l'homme

Surveillance of Social Media and International Human Rights

Présentée par :

Seán LOONEY

Direction de thèse :

Théodore CHRISTAKIS
PROFESSEUR DES UNIVERSITES, Université Grenoble Alpes — Directeur de thèse

Rapporteurs :

Marie-Laure BASILIEN-GAINCHE
PROFESSEUR DES UNIVERSITES, Université de Lyon
Yvonne MCDERMOTT-REES
PROFESSEUR, Swansea University
Darragh MURRAY
Dr, Queen Mary University

Thèse soutenue à huis clos le **16 mars 2023**, devant le jury composé de :

Marie-Laure BASILIEN-GAINCHE PROFESSEUR DES UNIVERSITES, Université de Lyon	Rapporteure
Yvonne MCDERMOTT-REES PROFESSEUR, Swansea University	Présidente, Rapporteure
Daragh MURRAY DOCTEUR EN SCIENCES, University of Essex	Rapporteur
Fabien TERPAN MAITRE DE CONFERENCES, UNIVERSITE GRENOBLE ALPES	Examinateur

Abstract

Bulk surveillance powers appear to be simultaneously contravening the general principles of European human rights law while being accepted as necessary by the jurisprudence the ECtHR and CJEU. This thesis illustrates this issue by analysing the UK Investigatory Powers Act 2016 as an example. Touted as the example for a modern bulk surveillance apparatus, the IPA instead shows how the human rights protection provided by the ECtHR and CJEU does not adequately protect against the dangers of bulk surveillance. This thesis first provides the legislative history and framework for the IPA before providing an analysis of the bulk surveillance powers described in the IPA, focusing on how they are described in the legislation, how they work in practice and what harms they incur. The takeaways from these analyses are two-fold. First, the harms caused by the use of these bulk powers goes beyond harms to privacy. Bulk powers also impact on freedom of expression and freedom of assembly. Second, each of these bulk powers operates in a qualitatively different way and thus the level of protection provided by safeguarding must be tailored to each individual power. These chapters are complemented by an analysis of the ECtHR's approach to bulk interception caselaw, and the CJEU's approach to data retention caselaw. These chapters find that both the ECtHR and CJEU allow for the use of bulk surveillance powers but limit their use through the use of required levels of safeguarding. Given the wide scope of harms caused by these bulk powers these safeguards aren't sufficient. Returning to the IPA, the thesis presents the case that the authorisation procedures, supervision and review mechanisms contained within the legislation cannot account for the harms caused by the use of these bulk powers while simultaneously being likely to be judged as compatible with the ECHR and EU law. Finally, the thesis proposes possible improvements for the IPA's legislative framework.

DECLARATION

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed .....  ..... (candidate)

Date .....29/09/2023.....

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s).

Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed .....  ..... (candidate)

Date ..... 29/09/2023.....

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed .....  ..... (candidate)

Date ..... 29/09/2023.....

Contents

List of Figures and Tables

List of Abbreviations

BA: Bulk Acquisition

BEI: Bulk Equipment Interference

BI: Bulk Interception

BPD: Bulk Personal Datasets

CSP: Communications Service Provider

CMP: Closed Material Procedure

CNE: Computer Network Exploitation

DPI: Deep Packet Inspection

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

ETF: Electronic Test Facility

GCHQ: Government Communications Headquarters

GDPR: EU General Data Protection Regulation

HRA: Human Rights Act

IPA: Investigatory Powers Act 2016

IPC: Investigatory Powers Commissioner

IPCO: Investigatory Powers Commissioners Office

IPT: Investigatory Powers Tribunal

JC: Judicial Commissioner

MVR: Massive Volume Reduction

NCND: Neither Confirm Nor Deny

NSA: National Security Agency

POAC: Proscribed Organisation Appeal Commission

PII: Public Interest Immunity

RIPA: Regulation of Investigatory Powers Act 2000

SIAC: Special Immigration Appeals Commission

TOR: The Onion Router

Acknowledgements

With utmost gratitude to my supervisors, Dr Katy Vaughan, Professor Stuart Macdonald, Professor Théodore Christakis and Dr Karine Bannelier for their invaluable support and constant guidance throughout this process.

Without the patience and support of my wife, Christie, undertaking the work for this thesis would not have been possible.

To my parents for raising and supporting me throughout my life, and my in-laws for taking me into their home during a pandemic.

My deepest thanks for the financial support from Université Grenoble Alpes and Swansea University which made pursuing this PhD possible.

In acknowledgement of all those who have supported me both professionally and personally throughout my early career.

1. Introduction

In 2013 National Security Agency computer intelligence consultant Edward Snowden provided thousands of documents to journalists Glenn Greenwald and Laura Poitras to be published by Wikileaks. At least 58,000 of these documents concerned "highly classified UK intelligence documents" and many of the published documents and slides referred specifically to GCHQ.[1] The intention behind Snowden's actions can be seen here:

> The shock of this initial period [after the first revelations] will provide the support needed to build a more equal internet, but this will not work to the advantage of the average person unless science outpaces law. By understanding the mechanisms through which our privacy is violated we can win here.[2]

While the shock of this initial period post revelations has dissipated in the nine years following the first Snowden revelations, a more equal internet has not materialised. While there has been a shift in public opinion and discourse on surveillance, it has led primarily to an acceptance of surveillance practices as a necessity of life.[3] Part of this process of acceptance has been the reform of these surveillance practices as part of the implementation of the Investigatory Powers Act 2016 (IPA). The IPA aimed to reform the previous primary statute for surveillance - the Regulation of Investigatory Powers Act 2000 - in the aftermath of the Snowden revelations, as well as several challenges at the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) level. The history of the IPA gives rise to two primary questions. The first is whether this new legislation addresses the issues with its predecessor and is thus compatible with European human rights law. The second is whether said European human rights law is capable of protecting against the harms of bulk surveillance.

Chapter 1 serves as an introduction to this thesis. It will begin by providing a background to the topic of bulk surveillance and the IPA, and the motivation behind the study of the compatibility with Article 8 ECHR. Following this the chapter outlines the research

[1] David Anderson, *A Question of Trust - Report of the Investigatory Powers Review* (2015).
[2] Glenn Greenwald, *No place to hide: Edward Snowden, the NSA, and the US surveillance state* (Macmillan 2014) p 13.
[3] Nik Thompson and others, 'Cultural factors and the role of privacy concerns in acceptance of government surveillance.' (2020) 71 Journal of the Association for Information Science and Technology 1129.

statement, and the core research objectives that flow from the central hypothesis of this thesis before presenting this thesis' claim to originality. The chapter concludes by outlining the methodological approach taken to this doctoral research and the structure of the thesis that is to follow.

1.1 Background and Motivation

One of the most prominent developments post-Snowden has been a clarification of terms, rather than the blanket descriptor of "mass surveillance" official sources have instead opted for "bulk surveillance". Bulk surveillance is a term which refers to several different practices. The clearest definition of bulk surveillance is that it involves the large-scale collection, retention and subsequent analysis of communications data.[4] Bulk surveillance has a basis in both UK national law[5] and international human rights law.[6]

The use of bulk surveillance by the UK Government, amongst others has been justified by multiple sources. In his Review of the Bulk Powers, then Independent Reviewer of Terrorism Legislation David Anderson Q.C. justified their use as such:

> The threat of terrorist atrocities curtails normal activities, heightens suspicion, promotes prejudice and can (as the terrorist may intend) do incalculable damage to community relations. A perception that the authorities are powerless to act against external threats to the nation, or unable effectively to prosecute certain categories of crime (including low-level crime), can result in hopelessness, a sense of injustice and a feeling that the state has failed to perform its part of the bargain on which consensual government depends.

A similar logic can be found in the European Court of Human Rights (ECtHR) with an important addendum:

> the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the

[4]Daragh Murray, and Pete Fussey, 'Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data.' (2019) 52 Israel Law Review 31 https://www.cambridge.org/core/journals/israel-law-review/article/bulk-surveillance-in-the-digital-age-rethinking-the-human-rights-law-approach-to-bulk-monitoring-of-communications-data/AA032EBA3EC3889D27054011853E5E59/core-reader

[5] Investigatory Powers Act 2016 Part 6.

[6] *Weber and Saravia v Germany* (2008) 46 EHRR SE5, *Big Brother Watch and Others v. The United Kingdom,* App nos. 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018).

> seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.[7]

While the Investigatory Powers Act 2016 forms the focus of this thesis, it is a successor to the Regulation of Investigatory Powers Act 2000. At the time of its implementation RIPA complemented and underpinned considerable investment in surveillance technology by the then UK Labour government. The legislation provided surveillance powers to a wide variety of public agencies including SIAs, police, local councils, environmental agencies, the Gambling Commission and the Food Standards Authority. While the intention was that these powers were only to be used to prevent and investigate serious crime and terrorism, in practice these powers were used for less pressing social issues such as benefit fraud and dog fouling.[8]

Public and media outrage following the Snowden revelations in 2013 prompted a number of reviews into the way the surveillance powers under RIPA were used by public authorities and how they should be regulated.[9] The most prominent of these reviews was *A Question of Trust* by then Independent Reviewer of Terrorism Legislation David Anderson QC. Anderson's review ended by recommending that new legislation regulating the use of these powers should ensure the privacy of communications, the prohibition of their use by public authorities (unless on specified terms), and judicial, regulatory, and parliamentary mechanisms for authorisation, audit and oversight of such use.[10]

The first draft of the Investigatory Powers Bill was presented in November 2015, with the proposed first reading of the Bill in February 2016. This left MPs, NGOs, and parliamentary

---

[7] *Big Brother Watch and Others v. The United Kingdom* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018) para 308

[8] Burkhard Schafer, 'Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill.' (2016) 40 Datenschutz und Datensicherheit-DuD 592

[9] Investigatory Powers Commissioner's Office 'History' https://www.ipco.org.uk/investigatory-powers/history/#:~:text=2000,as%20CHIS)%20by%20public%20authorities accessed 14/03/22

[10] David Anderson, *A Question of Trust - Report of the Investigatory Powers Review* (2015).

committees with an inordinately short period with which to analyse and respond to a 200 page Bill with 400 further codes of practice.[11] Nonetheless the draft bill was subject to extensive criticism from a variety of sources. The Joint Select Committee for the Investigatory Powers Bill, the committee charged with conducting public consultation on the Bill, received 148 separate submissions.[12]

The Investigatory Powers Act 2016 has yet to meet formal challenge at the ECtHR. RIPA has been subject to challenges in the European Court of Human Rights on multiple occasions, starting with *Liberty v United Kingdom* in 2009 where several civil liberties organisations alleged that their electronic and telephone communications were intercepted by the Ministry of Defence.[13] In *Kennedy v United Kingdom* the applicant had previously been convicted of manslaughter and alleged that his mail, telephone and email communications were being intercepted.[14] Finally, the most prominent challenge was in *Big Brother Watch v United Kingdom* in 2018[15] and the Grand Chamber judgment in 2021.[16] In each of these judgments RIPA has been subject to criticism by the Court, leading to the GC *Big Brother Watch* judgment where the Court found that RIPA was incompatible with Article 8 ECHR. However, throughout the *Big Brother Watch* judgments both the Court and UK Government referred to the newly implemented Investigatory Powers Act 2016 which amended the flaws the Court found with RIPA. This open question of whether the IPA does amend the flaws found with RIPA satisfactorily forms the basis of this thesis.

1.2 Thesis Statement and Objectives

The central aim of this thesis is to answer two primary research questions:

1. Are the bulk surveillance powers contained within the Investigatory Powers Act 2016 compatible with European Human Rights Law?
2. Is the level of protection provided by European Human Rights Law capable of protecting against the harms of bulk surveillance?

[11] Burkhard Schafer, 'Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill.' (2016) 40 Datenschutz und Datensicherheit-DuD 592
[12] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill: Report*, 2016 p26
[13] *Liberty v United Kingdom* (2009) 48 EHRR 1
[14] *Kennedy v United Kingdom* (2011) 52 EHRR 4
[15] *Big Brother Watch and Others v. The United Kingdom* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018)
[16] *Big Brother Watch v United Kingdom (GC)* App nos 58170/13, 62322/14, 24960/15 (ECtHR 25 May 2021)

Three core objectives flow from this position. The first is to provide a clear picture of the operation of bulk surveillance in the UK both in terms of the overall harms stemming from the use of these powers and how these powers differ from each other. Thus far discussions about the compatibility of bulk surveillance have falsely equated bulk interception with bulk surveillance. Bulk interception is simply one bulk surveillance power which can be used in a bulk surveillance regime. To fully evaluate the compatibility of these various powers, a clear picture of their operation and thus their impact on human rights is required. This thesis aims to provide this picture by utilising a mix of official and unofficial sources and in doing so provide a stable base for further doctrinal analysis.

Second, this thesis provides an analysis and critique of the protection provided by European human rights law against the harms of bulk surveillance. The thesis first examines ECtHR's Article 8 jurisprudence in relation to surveillance and bulk surveillance, with reference to national security and the covert nature of surveillance. The first component of this objective is to provide an analysis of the development of the test for compatibility with Article 8 in the context of surveillance regimes. The set of minimum requirements set out in *Weber and Saravia v Germany* have been repeatedly used and developed as targeted surveillance cases have given way to bulk surveillance cases. This is problematic as these requirements were developed in the context of targeted surveillance and as such do not reflect the reality of bulk surveillance powers. The second component concerns the latest development of the Court's approach, the so-called transition towards 'end-to-end' safeguards as a minimum requirement test. This thesis provides a critique of these new requirements along two lines. The first will show that these new requirements are just a modification of the *Weber* requirements and thus subject to the same problematic nature as their predecessors. The second will show how these 'end-to-end' safeguards overly focus on the ex-ante and ex-post stages of the operation of a bulk surveillance warrant, to the detriment of the examination and aggregation stage. This will be shown to be problematic as the real impact on Article 8 rights can occur at this stage depending on which bulk surveillance power is utilised. This examination of the ECtHR will be complemented by an analysis of the CJEU's caselaw on data retention as it provides a rich analysis of a method of bulk surveillance which has not been addressed by the ECtHR, bulk acquisition.

Finally, this thesis provides analysis and critique of the safeguarding under the Investigatory Powers Act. This analysis will initially focus on the homogenous application of safeguards to qualitatively different surveillance powers. Following this, each of the primary end-to-end

safeguards present in the IPA is critically evaluated. The bulk of this analysis is concerned with the system of judicial authorisation under the so-called "double-lock" warrant authorisation system, and the Investigatory Powers Tribunal as an ex-ante safeguard and domestic remedy. It will be demonstrated that the key challenge in both safeguards stems from the covert nature of surveillance.

1.3 Originality

This chapter presents the claims to originality as existing on three levels. The first is the level of surveillance practice and technology. Despite the time passed since the Snowden revelations and the subsequent discourse surrounding government use of surveillance, there hasn't been much of an attempt to synthesise a clear picture of how the UK surveillance regime operates in practice. The second, is at the ECHR level. There is an existing body of work on both the ECHR and Article 8. This thesis aims to contribute to this field by shifting the focus of the debate surrounding the compatibility of surveillance measures, and other national security measures, from the margin of appreciation to a more nuanced understanding of the test for adequate and effective safeguards against abuse. Finally, the third level of originality is the legislative level within the UK. Since its enactment the IPA has been subject to a variety of academic literature which has largely focused on the broad powers and their impact on society and civil liberties. Largely absent from this literature is a systematic critique of the safeguards present in the legislative framework which this thesis aims to contribute. In particular, this thesis provides a systematic critique of the flaws in the IPA's celebrated double-lock warrant system and a procedural justice analysis of the Investigatory Powers Tribunal which shows its flaws as an effective domestic remedy and a review mechanism for the IPA.

Research examining the use of bulk surveillance powers has focused primarily on estimating how they function in practice, despite their covert nature. Cayford et al in the aftermath of the Snowden revelations provided an initial classification of NSA surveillance technology, dividing them into technological categories. These included wiretaps, fiber-optic cables, fiber-optic splitters, deep packet inspection, PRISM, decryption, exploitation, analysis and databases.[17] Van der Velden provides a similar account of devices for data collection used by

[17] Michelle Cayford, Coen Van Gulijk and Pieter Van Gelder, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014)

the NSA.[18] Cayford and Pieters analysed US and UK intelligence official's statements as to their views on the effectiveness of surveillance technology over the course of 2006 to 2016. One of the key findings drawn from these statements is that it is extremely difficult to evaluate the effectiveness of surveillance programs. This is attributed to a number of sources such as intelligence work being akin to putting together pieces of a puzzle where multiple seemingly insignificant parts come together to form an important and critical picture.[19] In another study Cayford examines how oversight bodies evaluate the effectiveness of surveillance technology by SIAs along three lines: effectiveness, cost and proportionality. Measures of effectiveness included thwarted plots, knowledge gained, speed, reports and validating and prioritizing information. Whereas cost evaluation depends primarily on cost to value considerations. Oversight bodies ultimately "rely on judgments of proportionality to help determine legality, while intelligence practitioners demonstrate the reverse, relying on the law to determine proportionality."[20] Stella-Bourdillon et al attempt to place a finer point on discussions of the bulk collection of communications data by developing a more accurate framework for understanding differing forms of data. Rather than a simple binary of content versus communications data, they argue for three categories, network level metadata, application level metadata and service use metadata.[21] This thesis contributes to this area by clarifying bulk surveillance in operation within the UK context.

In their analysis of the surveillance law principles of the ECtHR, Galetta and De Hert explore complementing them with environmental law principles through an integrated technology approach. The authors explore how the ECtHR has developed a set of principles from Article 8 ECHR to counter both privacy and environmental interferences but apply them in different ways and generate difference species of legal protections. The authors argue for a harmonised approach between the two as the normative framework that applies to surveillance is evolving and is need of new regulatory paths. The principles which govern environmental interferences such as access to information, public participation in decision-making and

[18] Lonneke Van der Velden, 'Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance' (2015) 13 Surveillance & Society 182

[19]Michelle Cayford and Wolter Pieters, 'The effectiveness of surveillance technology: What intelligence officials are saying ' 34 The Information Society 88

[20] Michelle Cayford, Wolter Pieters and Constant Hijzen, 'Plots, murders, and money: oversight bodies evaluating the effectiveness of surveillance technology' 33 Intelligence and national security 999

[21] Sophie Stalla-Bourdillon, Evangelia Papadaki, and Tim Chown. "Metadata, traffic data, communications data, service use information… What is the difference? Does the difference matter? An interdisciplinary view from the UK." In Serge Gutwirth, Ronald Leenes, and Paul Hert (eds), *Data Protection on the Move*, pp. 437-463. (Springer Dordrecht 2016).

access to judicial review are argued to be invaluable to the current ECtHR approach to surveillance.[22] Fura and Klamberg conducted a comparative analysis of electronic surveillance laws in Europe and the USA, finding that the Fourth Amendment of the US constitution offers a greater protection than Article 8 ECHR to the extent that searches and seizures require probable cause and a warrant. However, this has led to US authorities to use warrantless surveillance or to define the notions of "search" and "seizure" more narrowly. The protection offered by the US constitution is then "all or nothing" whereas the ECHR has a broader scope.[23] Bygrave examined the extent to which the basic principles of data protection laws may be read into provisions in human rights treaties proclaiming a right to privacy, such as Article 8 ECHR. The author concluded that at time of writing the case law fsurrounding Article 8 falls short of explicitly stipulating data protection guarantees. Even with the relatively extensive body of relevant case law developed around Article 8, the principles for processing personal data which emerge from it are often sketch and of little prescriptory value.[24] However this may be due to the Court's practice of deciding based on the circumstances of the specific case before it.

Hughes provides a short account of the development of the ECtHR's case-law post Snowden revelations, arguing that the wide margin of appreciation granted to states in *Big Brother Watch v United Kingdom* undermines the important role the ECtHR has played in protecting individual rights. This wide margin of appreciation is argued by Hughes to allow states to use bulk surveillance and invoke the threat of terrorism seemingly without scrutiny.[25] Yourow takes a similar line in regard to the margin of appreciation doctrine in general, stating that the Court is always prepared to approve rights restrictive state action as falling within the wide margin of appreciation states enjoy as aspect of sovereignty in the national security context.[26] This appears to be in conflict with the Court varying the size of the margin of appreciation it affords states on a case by case basis. McHarg takes a more nuanced position here pointing

[22] Antonella Galetta and Paul De Hert, 'Complementing the surveillance law principles of the ECtHR with its environmental law principles: An integrated technology approach to a human rights framework for surveillance' (2014) 10 Utrecht Law Review 55

[23] Elisabet Fura and Mark Klamberg, The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA (October 23, 2012). Josep Casadevall, Egbert Myjer, Michael O'Boyle (eds), *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights* (Wolf Legal Publishers 2012) pp. 463-481

[24] Lee Andrew Bygrave, 'Data protection pursuant to the right to privacy in human rights treaties' (2008) 6 International Journal of Law and Information Technology 247

[25] Kirsty Hughes, 'Mass surveillance and the European Court of Human Rights' (2018) 6 EHRLR 589

[26] Howard Charles Yourow *The margin of appreciation doctrine in the dynamics of European human rights jurisprudence* (Martinus Nijhoff Publishers 1996). p. 107

towards the indeterminacy at play when the Court encounters a case where both the public interest and the impact of the interference on the right are seen as important.[27] This thesis adds to this body of work by shifting the focus in the context of national security and surveillance from the wide margin of appreciation to the specific test of adequate and effective safeguards against abuse and the effect this has on the variable size of the margin of appreciation granted to states.

What literature there is discussing the IPA has taken a very critical position. Goodman utilises deliberative democracy theory in conducting a democratic critique of the surveillance powers under the IPA. These broad investigatory powers are argued to erode essential boundaries between public and private spheres by compromising populations' ability to freely communicate. In doing so these powers erode the legitimacy of democratic processes and institutions.[28] Similarly Murphy argues through an historical analysis that social democrats, such as the Labour Party, are failing to address threats to civil liberties.[29] Boukalas argues that the logic of intelligence contained within the IPA is incompatible with the rule of law.[30] Waranach's work examines how the bulk acquisition warrant provisions contained within the IPA are incompatible with the Charter of Fundamental Rights of the European Union.[31] In their evaluation of the potential harm caused by bulk communications data surveillance, Murray and Fussey argue for the importance of defining specific offences to which bulk surveillance may be applied. They take a nuanced approach in arguing that these offences should be limited to activities that constitute a genuine threat to democratic institutions, where the use of such broad powers are warranted.[32] While the IPA is used as an example of modern domestic legislation that regulates surveillance practices, the authors add that the article does not intend to analyse the IPA or its compliance with the requirements of

[27] Aileen McHarg, "Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights" (1999) 62(5) M.L.R. 671 at 677.
[28] Tristan Goodman, 'The Investigatory Powers Act 2016: A Victory for Democracy and the Rule of Law' (2018) 5 Bristol Law Review 2
[29] Cian Murphy, 'State Surveillance and Social Democracy' in Alan Bogg, Jacob Rowbottom and Alison Young (eds), *The Constitution of Social Democracy* (Hart Publishing 2020)
[30] Christos Boukalas, 'Overcoming liberal democracy: "Threat governmentality" and the empowerment of intelligence in the UK investigatory powers Act' 82 Studies in Law, politics, and society 1
[31] Rubin Waranch, 'Digital Rights Ireland Deja Vu: Why the Bulk Acquisition Warrant Provisions of the Investigatory Powers Act 2016 Are Incompatible with the Charter of Fundamental Rights of the European Union' 50 George Washington International Law Review 209.
[32] Daragh Murray, and Pete Fussey, 'Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data.' (2019) 52 Israel Law Review 31 https://www.cambridge.org/core/journals/israel-law-review/article/bulk-surveillance-in-the-digital-age-rethinking-the-human-rights-law-approach-to-bulk-monitoring-of-communications-data/AA032EBA3EC3889D27054011853E5E59/core-reader.

human rights law.[33] This thesis contributes to this field by shifting the focus of the analysis from the broad powers towards the safeguards present in order to minimise the potential impact of said powers on individuals' rights.

In line with this refocusing, this thesis contributes to the literature surrounding the Investigatory Powers Tribunal. Since its inception the IPT has been subject to extensive criticism. Kavanagh analyses how the "Neither Confirm Nor Deny" policy of the UK government in regards to surveillance leaves the IPT without sure footing to challenge the executive on these matters.[34] Hickman discusses the effect of the, since removed, ouster clause effectively removing the IPT from the supervision of higher courts.[35] Wilson provides a thorough analysis of the IPT as it developed over the course of two decades. While the Tribunal is seen to have undergone significant procedural development since its inception, it is uncertain in their view whether the reforms have plateaued. Wilson highlights significant concerns of fairness in its procedure.[36] This thesis then complements this work by providing a procedural justice analysis of the IPT's caselaw.

The other primary safeguard of the IPA, the so-called double-lock system, is more recently introduced than the IPT and as such has been subject to less analysis. Davies examined the role of the new IPA provisions, including the double-lock, in policing the Dark Web.[37] Scott provides the most thorough evaluation of the double-lock thus far in his work evaluating the Judicial Commissioners as a hybrid institution which marry certain features characteristic of political institutions with those of legal institutions. Scott argues that these commissioners represent a new phase in the development of the institutional facets of the national security constitution as the JCs carry out a wider range of functions than their predecessors. The JCs also operate in a public awareness of national security operations which is much broader than predecessors In this way the minimalist approach taken by previous incarnations of commissioners is no longer viable for the JCs, and the institution is more valuable as a result.[38] To Woods the Judicial Commissioners also operate in a dual role wherein they blur

[33] Ibid.
[34] Aileen Kavanagh, 'Constitutionalism, Counterterrorism, and the Courts: Changes in the British Constitutional Landscape' (2011) 9(1) IJCL 172, p. 178.
[35]Tom Hickman "The Investigatory Powers Tribunal: a law unto itself?." *Public Law* 2019 (2019): 584-594.
[36] Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129
[37] Gemma Davies, 'Shining a light on policing of the dark web: an analysis of UK investigatory powers' (2020) 84 The Journal of Criminal Law 407
[38] Paul F Scott, 'Hybrid institutions in the national security constitution: the case of the Commissioners.' 39 Legal Studies 432

the boundary of regulatory and judicial oversight. The judicial commissioners oversee aspects of surveillance using an oversight model that is regulatory but which is reliant on judicial independence.[39]

This thesis also contributes to the vast literature on appropriate deference in judicial review in a national security context, through its analysis of the how the Judicial Commissioners will likely review warrants as part of the so-called double-lock system. Kavanagh examines how the *Belmarsh* decision rejected the idea that the courts should adopt a completely hands-off approach to executive decision making in this arena.[40] As stated by King, the notion of national security being a judicial no-go area was replaced by a "more flexible and pragmatic test of deference."[41] As shown by Scaramuzza this does not mean that the courts will never take a highly deferential position.[42] Still, the stance taken by the House of Lords in *Belmarsh* has filtered to the lower courts. Tomkins demonstrates how this occurred in the Administrative Court, Special Immigrations Appeals Commission and the Proscribed Organisation Appeal Commission.[43] On top of the theoretical implications outlined above this thesis also provides a number of policy implications for the IPA legislative framework which are detailed in the conclusion.

1.4 Methodology and Thesis Structure

Due to the covert nature of surveillance this thesis focuses primarily on the legislative framework for the operation of the legislation, as opposed to the operation of the legislation itself. In line with this a doctrinal approach to research is employed. The approach employed here does not limit itself to a simple discussion of what the law is, its compatibility in terms of current ECHR and CJEU jurisprudence, and how the powers described under the IPA are utilised. Rather it will aim to extract wider theoretical arguments on this topic. The employment of a doctrinal approach does not imply that other approaches to research in this area have less value. Going forward the examination of how bulk powers operate in practice in combination with the safeguards present in the IPA will be invaluable to evaluating the

[39] Lorna Woods, Lawrence McNamara, Judith Townend, 'Executive Accountability and National Security' (2021) 84 Modern Law Review 553

[40] Aileen Kavanagh, 'Constitutionalism, Counterterrorism, and the Courts: Changes in the British Constitutional Landscape' (2011) 9 International Journal of Constitutional Law 172.

[41] Jeff King, 'The Justiciability of Resource Allocation' (2007) 70 Mod. L. Rev. 198 p 224

[42] T Scaramuzza, 'Judicial deference versus effective control: the English courts and the protection of human rights in the context of terrorism' [2006] 11 Coventry Law Journal 2, 10

[43] Adam Tomkins, 'National Security and the role of the court: a changed landscape?' (2010) 126 LQR. 543-567,

levels of harm caused by the use of bulk powers as well as the level of protection provided by European human rights law. This research will form a basis for further research into the safeguarding of bulk powers, the demand for which will only grow as more cases concerning bulk surveillance and the IPA come before national and supranational courts.

The research for this thesis was conducted in primarily three stages. The first stage was to build an analysis of how bulk surveillance powers operate in practice within the UK surveillance regime. This enabled the identification of flaws within the legislative framework governing their use. Stage one involved a review of the academic literature on the operation of surveillance systems, evidence adduced as part of surveillance cases, leaked material derived from the Snowden revelations, and official sources on how bulk surveillance is conducted within the UK. The comparing and contrasting of these sources' accounts of bulk surveillance enabled the identification and categorisation of various bulk powers of surveillance rather than a single broad category of bulk surveillance. This was important as it contextualised the operation of the bulk surveillance regime and enabled the construction of a more nuanced critique of the IPA.

The second stage of research was a systematic analysis of the ECtHR's Article 8 jurisprudence and the CJEU's jurisprudence on data retention, focusing primarily on each Courts' approach to the compatibility of surveillance regimes in order to examine the compatibility of the IPA. This second stage included the interpretation of the ECHR in this context and enabled a rigorous review of the ECtHR's approach to the justification of surveillance regimes under Article 8(2). This analysis of the ECtHR is complemented by an analysis of the CJEU's caselaw on data retention in order to provide a fuller picture of the compatibility of the IPA with European human rights law as well as the level of protection provided by said caselaw.

The third stage of research was informed by stages one and two. Utilising the clear picture of how bulk surveillance is conducted in combination with the Court's approach to justifying the use of bulk surveillance regimes, the third stage is a thorough analysis of each aspect of the IPA as embedded within the UK legal system. This involved a review first of the legislation itself, its supplementary codes of practice, reports by oversight bodies, and academic literature. As a thorough accounting of the legislation gave way to critique and analysis of specific safeguards present, more specific lenses of analysis were incorporated into the research. For the portion of research evaluating the judicial authorisation present in

the so-called double-lock system, an analysis of the appropriate role of the judiciary, judicial standard of review, and the appropriate deference granted within the national security context was required. For the portion of research evaluating the Investigatory Powers Tribunal as a domestic remedy, an analysis of both the substantive justice drawn from reporting and caselaw, as well as a critique utilising notions of procedural justice and fairness was required.

The structure of this thesis is, in part, a reflection of the methodology. Chapter 2 aims to provide context for the thesis by setting out both the IPA legislative framework and its legislative history. It shows how the UK legislation has provided SIAs with updated powers that are fit for the modern age and contemporary forms of communications. However, the implementation of human rights safeguards has failed to keep pace with the creation and the practical realities of these new powers, in at least three respects. First, the definition of key terms, and therefore the scope of the powers, are an awkward fit for modern forms of communications. Second, there are significant differences between the powers conferred by the legislative framework, yet the safeguards largely apply homogenously, meaning that they are ill suited to some of the powers in question. Third, the safeguards largely apply ex-ante and ex-post with insufficient oversight at the crucial selection for examination stage.

Chapter 3 provides the framework for the analysis of the compatibility of surveillance operations by outlining Article 8 ECHR, and in doing so outlines the Court's approach to targeted surveillance. Following this the chapter discusses how the covert nature of surveillance in combination with developments in technology has placed the Court's approach in a difficult bind. This is part of a larger trend which is explored in subsequent chapters where the Court's historic approach to surveillance is not equipped for the demands of today both in terms of procedural and substantive principles.

Chapters 4 and 5 attempt to provide a clear picture of the operation of bulk surveillance in the UK context. Chapter 4 aims to provide a full framework for both understanding how bulk interception works and its potential harms. To do so it first sets out a typology of terms to understand bulk surveillance more generally, in line with this the chapter sets out what data the act of bulk interception does and doesn't collect. The chapter next provides a technological explanation of how the UK bulk interception regime functions based on a comparison of official and unofficial sources. With this understanding in mind the chapter concludes by providing an analysis of the harms posed by bulk interception to privacy, freedom of expression and freedom of assembly. The scope of bulk interception and the

harms posed by its use provides a uniquely difficult issue for human rights bodies such as the ECtHR and the CJEU to protect against, one which they may not be able to deal with. Chapter 5 builds on this by comparing and contrasting the remaining bulk surveillance powers available under the IPA with bulk interception in order to show how each bulk surveillance power differs from the other in terms of both operation and harm. The principal way this is done is through the comparison of the Snowden Leaks and more official narratives. Due to the clandestine nature of surveillance this chapter aims to use this mix of sources to construct as clear a picture as reasonably possible of the bulk surveillance operation. It also draws on academic commentary in its aim to provide as clear a picture of this subject as possible. This is supported by a discussion on the nature of metadata which goes beyond more reductive definitions proposed by the UK Government.

The thesis then shifts its focus to European human rights law on surveillance. Chapter 6 builds on the findings of article 3 by examining the development of the ECtHR's case law on surveillance as target surveillance cases gave way to bulk interception cases. This chapter ends with a critical analysis of the Court's recent development of 'end-to-end' safeguards. Chapter 7 aims to complement the ECtHR's focus on bulk surveillance cases in chapter 6 with an analysis of the CJEU's caselaw on data retention which has direct applicability to the bulk acquisition power under the IPA. This chapter aims to show how, while the initial impression of the CJEU caselaw is stricter than the ECtHR's, the CJEU's approach has softened over time to directly resemble the ECtHR's approach. Both allow for the use of bulk surveillance regimes for the purposes of national security, provided certain minimum requirements against abuse are met.

Chapters 8 and 9 then shifts the thesis' focus back to the UK legislative regime on bulk surveillance, specifically the authorisation mechanisms and the review and oversight mechanisms contained within the IPA. The two chapters examine these ex-ante and ex-post safeguards emphasised by the ECtHR in chapter 6 as 'end-to-end' safeguards in turn. Chapter 8 focuses primarily on the so-called "double-lock" system of independent ex-ante authorisation under the Investigatory Powers Act. The analysis built in this chapter focuses on four major aspects: the appropriate role of the judiciary in this national security context, the likely standard of review the JCs will apply, the deference that these JCs will afford to the executive, and the impact of institutional factors on how the JCs operate. Chapter 9 then evaluating the review mechanisms and oversight present in the IPA regime; namely the auditing and inspections conducted by the Investigatory Powers Commissioners Office

(IPCO), the annual reporting done by the IPCO, and the Investigatory Powers Tribunal (IPT). This chapter builds a sustained critique of the IPT from a procedural justice perspective, as a substantive justice perspective is difficult due to the inherently covert nature of the material the IPT deals with. Following this critique the chapter examines comparators for the IPT in Public Interest Immunity and Special Advocates. The chapter then finishes by drawing recommendations from these comparators as to how the IPT can be improved. Each of these chapters come to the same conclusion, that the relevant safeguards present in the IPA are deeply flawed and unable to protect against the harms of bulk surveillance. Yet they are likely to be considered compatible with European human rights law. The thesis concludes by outlining the theoretical and policy implications of these findings, showing how the IPA regime can be reformed in order to improve the level of protection provided against the harms of bulk surveillance.

2. Legislative History and Framework of the Investigatory Powers Act 2016

The Investigatory Powers Act 2016 is the end product of a turbulent legislative process by the UK government to regulate the use of surveillance powers. This turbulent period began with the invalidation of the EU Data Retention Directive by the CJEU in *Digital Rights Ireland*. The Directive was the basis for one of the IPA's predecessors: the Regulation of Investigatory Powers Act 2000. This, combined with the visibility of state surveillance exposed by the Snowden leaks, led to the enactment of the Data Retention and Investigatory Powers Act (DRIPA) 2014 which was meant to address the shortcomings of RIPA. However this too was found to be 'not fit for purpose' following the CJEU's *Tele2 and Watson* judgment. In the domestic proceedings for *Watson* the High Court concluded that DRIPA was incompatible with EU as set out in *Digital Rights Ireland*. The reason being that the CJEU had found in that case that communications data retention was only permissible if the objective was to fight serious crime, a threshold not provisioned in DRIPA. While this judgment was appealed it became apparent that new legislation was needed to correct and expand upon DRIPA.

Section 7 of DRIPA required the then Independent Reviewer of Terrorism Legislation, David Anderson QC to "review the operation and regulation of investigatory powers." [1] While DRIPA was quickly invalidated the report influenced the push towards a new legislative frame. The report proposed that:

> a comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive power that it may be necessary for public authorities to use.[2]

The draft Bill was published in November 2015, and a joint committee of the House of Commons and House of Lords was established to scrutinise the draft bill. The Joint Committee made 198 recommendations, the vast majority of which were accepted, and the revised bill was introduced to the Commons on the 1st March 2016 before receiving Royal Assent on the 29th November 2016. This chapter first sets out the legal basis for the bulk surveillance powers described previously in chapter 1 before discussing issues with

[1] David Anderson QC. *A Question of Trust – Report of the Investigatory Powers Review* (2015) p 10
[2] ibid

definitions and how they apply to modern social media platforms. Finally, the chapter outlines the regimes for bulk powers contained in the IPA 2016. Issues with the primary ex-ante and ex-post safeguards will be highlighted here before further examination in subsequent chapter.

2.1 First Debate in House of Commons

During the Parliamentary debates on the IPA it is possible to see a growing soft bipartisan consensus on the legitimate use of bulk powers.[3] This is seen in both the House of Commons and the House of Lords. The two largest parties, Labour and the Conservatives, have very similar positions on the necessity of these powers. The Draft Investigatory Powers Bill was first debated on Wednesday 4 November 2015.It is clear that the first round of IPA debates in the House of Commons were structured primarily by the opening statement of the then Home Secretary Theresa May and the first response by the opposition led by Andy Burnham, the then Labour MP for Leigh.

May's focus is first on the necessity of the surveillance powers contained within the IPA. While contemporary computing technologies and the internet have changed our lives for the better, the same benefits are "being exploited by serious and organised criminals, online fraudsters and terrorists."[4] May outlines how six terrorist plots were stopped in the 12 months leading up to this debate, cyber-attacks were increasing and there were an estimated 50,000 people downloading indecent images of children. Despite this necessity May emphasises that the Government is not simply providing unlimited powers to the police and intelligence and security agencies, but rather it is the role of Parliament and the Government to provide limits to these powers.[5]

When May introduces the bulk powers she is careful to emphasise that these are not new powers but rather the IPA is collecting disparate powers into one piece of legislation. The power chosen to highlight is bulk acquisition of communications data, replacing the power under Section 94 of the Telecommunications Act 1984. She highlights how bulk acquisition played a key role in stopping a terrorist attack in London in 2010: "it allowed investigators to

[3] Sotirios Santatzoglou, and Maria Tzanou. "An (In) Adequate Data Protection Regime after Brexit? Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers." *Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers (January 16, 2023). forthcoming in E. Celeste (et al.) Data Protection and Digital Sovereignty Post-Brexit (Hart, 2023)* (2023).
[4] HC Deb 15 November 2015, vol 601, cols 969-972.
[5] Ibid.

uncover the terrorist network and to understand their plans."[6] This is followed up by reminding the Commons of the robust safeguards and independent oversight of this power.

May then focuses her speech on the aforementioned limits to bulk acquisition. The first is that it does not include the content of communications or internet connection records, in other words browsing history. The second is that it will be subject to oversight by the new Investigatory Powers Commissioner (IPC), replacing the interception of communications commissioner, intelligence services commissioner and chief surveillance commissioner. The IPC is a senior judge "supported by a team of expert inspectors with the authority and resources to effectively, and visibly, hold the intelligence agencies and law enforcement to account. These will be world-leading oversight arrangements."[7]

This leads to the conclusion of the speech wherein the Home Secretary focuses on authorisation, specifically the double-lock warrant authorisation as "one of the most important means by which I and other Secretaries of State hold the security and intelligence agencies to account for their actions."[8] May draws on the three reports produced examining the UK surveillance legislative framework. In David Anderson QC's report he argued that judges should carry out the authorisation, RUSI argued that the authorisation of warrants should have a judicial element but that the executive should play an important role, while the Intelligence and Security committee maintained that authorisation should be conducted solely by the Secretary of State. It is within this context that the double-lock warrant system is proposed.

The opposition's response to this was to accept the framing of the necessity of these powers but to emphasize the need for correspondingly strong safeguards: "strong powers must be balanced by strong safeguards for the public to protect privacy and long-held liberties."[9] To this end Burnham accepts that the safeguards discussed by May are sufficient, particularly in the area of authorisation. He adds that he wishes for the IPA to not be known as a 'snoopers charter or a plan for mass surveillance. Burnham raises some concerns about data retention and storage, specifically referring to the possibility of data breaches of personal data in public and private bodies. He also raises the legitimate concerns of the Muslim community who fear that these surveillance powers will be used against them disproportionately. Finally, he

[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] HC Deb 15 November 2015, vol 601, cols 972-974

acknowledges that the issues the IPA seeks to tackle are difficult and go beyond party politics. He commits to inspecting and improving the safeguards but states that the Home Secretary has gotten the balance of national security versus privacy and liberty broadly correct.

2.2 The Joint Committee: A call for an operational justification of the bulk powers

In terms of the bulk powers in general, a number of witnesses were concerned about the lack of clarity as to the scope of the powers. Dr Paul Bernal stated that how bulky the bulk powers are is "largely a matter of speculation, and while that speculation continues, so does legal uncertainty."[10] The UN Special Rapporteur argued that the provisions on bulk interception warrants are vague and not tied to specified offences. This tied with the use of ambiguous terms such as "economic well-being" heightened the risk of excessive and disproportionate interception.[11] In line with this, witnesses were concerned with the lack of justification for these powers. The committee maintained that while the majority of witnesses were concerned with the lack of justification, they were all commenting on the basis of incomplete information owing to the covert nature of surveillance. They cited the positive findings of the ISC report which had full access to the powers. Still the Committee recommended that the government should publish a fuller justification for each of the bulk powers alongside the Bill, and that these justifying examples should be examined by an independent body such as the Intelligence and Security Committee or the Interception of Communications Commissioner.[12]

Witnesses had issues with each of the bulk powers individually as well. With bulk interception witnesses raised the lack of clarity surrounding the term 'related communications data'. Graham Smith suggested that the Home Office could clarify this by producing a comprehensive list of datatype examples.[13] The Open Rights Group expressed concern that communications data from intercepted communications was more amenable for automated analysis.[14] The Committee again cited the ISC report which suggested that automated analysis of communications data was the primary value of bulk interception.[15] This line of

[10] Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill Report* (HL Paper 93 HC 651 2016) para 312.
[11] Ibid para 313.
[12] Ibid paras 314 – 319.
[13] Ibid para 353.
[14] Ibid para 355.
[15] Ibid para 356.

concern continued with bulk acquisition. Witnesses claimed that communications data, when aggregated, are more revealing and intrusive than content data, that the distinction between content and communications data was meaningless. Communications data is hugely more valuable than content because it can be combined with other metadata. Content, by contrast, cannot be combined with other content automatically as computers cannot understand it. So the Government's suggestion that communications data is somehow less intrusive than content data is "not just wrong, but exactly wrong: it is hugely more intrusive, which is why it should never be gathered routinely, as proposed here."[16] The Committee agreed that communications data has the potential to be very intrusive and repeated its call for fuller justifications as to the necessity and appropriateness of these powers.[17]

Concerns were raised to the committee about the bulk equipment interference power. CSP's such as Facebook, Google, Microsoft, Twitter, and Yahoo submitted that they would have to weaken their systems in order to comply with EI warrants, adding that there were no statutory provisions relating to network integrity or cyber security.[18] Vodafone similarly pointed out the obligations faced by operators in the UK and EU to ensure the security of their networks and services. Other CSPs such as Apple and Virgin Media added that the role of CSPs in Equipment Interference isn't clear in the draft Bill. Big Brother Watch summed up these concerns: "given the clear risks involved, the proportionality of the tactic needs to be considered. Equipment interference should not be used as a bulk tactic designed to infiltrate broader systems, networks or organisations."[19]

Finally, concerns were raised as to the safeguards present in the draft Bill. Overall witnesses suggested that the safeguards for bulk powers were insufficient. These concerns included that there was nothing in the draft Bill which imposed any kind of upper limit on what might be obtained by way of a bulk warrant. The only requirement being that the Secretary of State considers it necessary in the interests of national security or one of the other specified interests.[20] The Equality and Human Rights Commission called for more attention to be given examination safeguards as well as retention and destruction of material safeguards.[21]

[16] Ibid para 360.
[17] Ibid para 362.
[18] Ibid para 365.
[19] Ibid para 363.
[20] Ibid para 343.
[21] Ibid para 344.

Dr Tom Hickman insisted that the Committee make three recommendations at minimum on this point. The first being tighter protections for persons in the UK, specifically in relation to the use of communications data "requiring at least operationally independent authorization for use of such data together with JC approval where this would be required for police obtaining communications data."[22] The second was to requiring warrants to be more narrowly focused as to their purpose and permitted search criteria. Finally, the third was to bring safeguards currently in the Code to legislation and other matters on record-keeping and destruction from internal policy to legislation.[23] However, the Committee stated that they were content that the safeguards proposed by the Home Office, buttressed by authorisation by Judicial Commissioners and oversight from the Investigatory Powers Commissioner would be sufficient to ensure the proportional use of the bulk powers.[24] The Committee did acknowledge the call for greater safeguards for bulk powers and repeated that it was difficult to make a thorough assessment of the effectiveness of further safeguards without a greater understanding of how the bulk powers operated in practice. The Committee recommended that the IPC, within two years of appointment, should produce a report on the existing safeguards and how they might be improved.[25]

2.3 Reporting Stage Debate of the IPB – 6/06/2016 – 7/06/2016

One of the most telling case studies of this bipartisan soft consensus on bulk powers comes from the reporting stage debate of the IPB.[26] Despite the IPB's huge constitutional importance, it was allocated "fewer than two full working days to debate it on Report."[27] It was here that a number of MPs from small opposition parties such as the Liberal Democrats and the Scottish National Party alongside a few Conservative and Labour backbenchers raised a number of criticisms of the bulk powers. These included Conservative MP McPartland who noted that "the carte blanche on bulk powers should not be the first resort; it

[22] Ibid para 345.
[23] Ibid.
[24] Ibid para 348.
[25] Ibid para 349.
[26] Sotirios Santatzoglou, and Maria Tzanou. "An (In) Adequate Data Protection Regime after Brexit? Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers." *Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers (January 16, 2023). forthcoming in E. Celeste (et al.) Data Protection and Digital Sovereignty Post-Brexit (Hart, 2023)* (2023).
[27] HC Deb 6 June 2016, vol 611, col 1148.

should always be the last resort."[28] The SNP MP McLaughlin used an offline analogy to highlight the invasiveness of bulk powers:

> "If we were asked by the state to deposit our membership forms for various organisations – political parties, campaign groups, golf clubs – or forms with our direct debit details, health records and other such bulk information into a big safe on the understanding that only the security services would have access to it, we would rightly baulk at such a proposal."[29]

McLaughlin added that the fact that such a system is online and without the consent of the individuals does not make it acceptable "in many ways, it makes it much worse."[30]

Nonetheless the position taken by the Labour Party was to take a reasonable and pragmatic approach to the bill.[31] In addition to Burnham's response to May's speech outlined above, throughout the process Labour were keen to be seen as working together on the Bill. Here at the Report Stage Labour MP Keir Starmer discussed the "good progress" made in the House on the bill.[32] Conservative MP James Berry described LD MP Carmichael's criticisms as a disappointing reaction to the "very constructive way" Andy Burnham had dealt with the Government.[33] The three key aspects of this reasonable and pragmatic approach were to suggest that (a) the Bill to incorporate an overarching privacy clause (b) to set an independent review of the operational case for the bulk powers and (c) to limit the definition of 'serious crimes' to cover offences with a provisioned imprisonment of more than six months.[34]

In regards to (a) the Government agreed to implemented the clause however in practice the clause had no binding effect on decision-makers.[35] The result of the clause was a clear statement about the importance of privacy, highlighting the question of 'whether what is sought to be achieved … could reasonably be achieved by any less intrusive means'[36] The section further highlights the sensitivity of any information sought and the public interest in

[28] HC Deb 6 June 2016, vol 611, col 1092.
[29] HC Deb 6 June 2016, vol 611, col 1058.
[30] Ibid.
[31] HC Deb 15 November 2015, vol 601, Column 952.
[32] HC Deb 6 June 2016, vol 611, col 1065.
[33] Ibid, col 1135.
[34] Sotirios Santatzoglou, and Maria Tzanou. "An (In) Adequate Data Protection Regime after Brexit? Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers." *Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers (January 16, 2023). forthcoming in E. Celeste (et al.) Data Protection and Digital Sovereignty Post-Brexit (Hart, 2023)* (2023).
[35] Lorna Woods, 'The Investigatory Powers Act 2016' (2017) 3 Eur Data Prot L Rev 13.
[36] S229 IPA

the integrity of communications and the protection of privacy. Crucially, the formulation requires that the relevant authority to 'have regard to' these issues rather than to require that these interests are respected.[37]

The Government also agreed to (b), to this end it was agreed for an independent review of the Bulk Powers would be undertaken by the then Independent Reviewer of Terrorism Legislation David Anderson KC. The findings of this review is discussed in the following section. Finally (c) Labour MPs' definition of "serious crimes", in other words the level of crime that bulk surveillance could be applied to, was to limit it to offence with a provisioned imprisonment of more than six months. This was explicitly stated to be proportionate by Andy Burnham MP. Two years later following the CJEU judgment in *Privacy International* the government conceded that this six month imprisonment threshold did not reflect the CJEU's notion of 'serious crime' and increased the threshold to 12 months.[38] The primary divide between the Government and Labour versus the smaller parties was the necessity of these powers.

2.4 Conclusions of the Independent Review

This divide led to Anderson's Report of the Bulk Powers Review which is invaluable to this thesis due to its privileged access to the UK bulk powers surveillance system and its attempt to assess the utility of these powers. The review is extensive and details and assesses each power in turn. However, the function of the review was not to pronounce on the overall case for bulk powers. Anderson was explicitly forbidden from considering the safeguards that apply to bulk powers and associated questions of proportionality, which was considered to be a matter of Parliamentary scrutiny.[39]

Anderson is clear on the potential harms of the assessed bulk powers, he describes them as "a human rights issue in relation to this Bill that dwarfs all others."[40] He attributes this to three distinct reasons. The first being that bulk powers, by definition, involve potential access to the "data of large numbers of people whom there is not the slightest reason to suspect of threatening national security or engaging in serious crime."[41] The second reason is that with

[37] Lorna Woods, 'The Investigatory Powers Act 2016' (2017) 3 Eur Data Prot L Rev 13.
[38] Home Office, Investigatory Powers Act 2016: Response to Home Office Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data (June 2018); White (n 8) 635,636
[39] Anderson para 1.11.
[40] Ibid para 9.6.
[41] Ibid.

this huge scope any abuse of those power could have particularly wide ranging effects on the innocent. Finally, the third reason was that even the perception that abuse is possible, and that it could go undetected, can generate a corrosive mistrust.[42] None of these factors are compelling reasons to renounce the use of bulk powers for Anderson. Rather, bulk powers should only be countenanced "if there is a compelling operational case for their use, and if their use is subject to adequate and visible safeguards."

Anderson is similarly clear on the utility of bulk powers. He makes the case that while alternative capabilities could sometimes be deployed, such as targeted versions of the powers or human agents, these alternatives would be slower, produce less comprehensive intelligence, were more dangerous, more resource-intensive or slower. Leading Anderson to the conclusion that there was simply no realistic alternative to use of the bulk power and in the majority of case studies reviewed, the contributions made by bulk powers could not have been replicated by other means.[43] This is as close as Anderson comes to making the claim that these powers are necessary rather than simply having utility. This is most likely due to his limitation by Parliament of making the operational case for these powers rather than discussing their necessity or proportionality.

As the making of recommendations in relation to safeguards was specifically excluded from the remit of the Review, Anderson makes just one: a Technology Advisory Panel. This panel would be appointed by and report to the Investigatory Powers Commissioner and advise the IPC and Secretary of State on the impact of changing technology on the exercise of investigatory powers. The panel would also advise on the availability and development of techniques to use those powers while minimising interference with privacy.[44]

Given the emphasis on limiting these powers with adequate and visible safeguards it is unfortunate that Anderson's review was prohibited from reviewing the safeguards or making any recommendations on them. While it was within Parliament's right to reserve scrutiny of safeguards, it could only have helped debates on these powers to have recommendations by someone who has had privileged access to how these powers operate in practice. The necessity and proportionality of these covert, intrusive bulk powers is inherently tied to the ability of safeguards to limit their use.

[42] Ibid.
[43] 9.14.(e)
[44] Paras 9.25 – 9.32.

2.5 Response to Anderson's Review

Responses to Anderson's Review were largely discussed in the House of Lords rather than the Commons. Upon the first reading of Anderson's report the debate centred on the addition of a new clause establishing Anderson's recommended Technology Advisory Panel. Baroness Hamwee summed up the frustration and confidence with Anderson: "There is so much confidence in him. We are all aware of the care that he has taken with this report and to stay within the terms of reference, which we, too, would have liked to have been rather wider."[45] Lord Campbell points out that the fact that the review does not reach conclusions as to the proportionality or desirability of the bulk powers.[46]

Earl Howe, the then Minister of Defence, outlined first that Anderson had shown and was limited to the utility of these bulk powers in his report. It was for Parliament to decide upon the correspondingly strong safeguards and that "the Government are clear that the Bill ensures that robust safeguards and world-leading oversight will apply to the exercise of bulk powers."[47] The example of this oversight and safeguarding:

> "Every bulk warrant will be subject to the double lock; any subsequent examination of material collected must be considered necessary and proportionate for an operational purpose approved by the Secretary of State and a judicial commissioner; and before issuing a bulk warrant, the Secretary of State must consider whether the same result could be achieved through less intrusive means."[48]

In the Commons Joanna Cherry MP criticised both the fact that Anderson's review reported to the House of Lords rather than the democratically accountable House of Commons. While she added that it was an excellent review, it is what is missing from the Review which is important: "It makes out a case that bulk powers can be of use to the state, but does not address the necessity and proportionality of those powers. These matters are yet to be addressed, and we will not get to debate them here."[49]

2.6 The need for broad but limited powers

[45] HL Deb 7 September 2016, vol 774, col 1047.
[46] Ibid, col 1051.
[47] Ibid, col 1053.
[48] Ibid.
[49] HC Deb 1 November 2016, col 616, col 852.

Throughout the parliamentary debates there is a clear focus on the need for these bulk powers and the utility they provide to SIAs. In the age of the internet, big data and world-wide social networks, the job of the intelligence and security agencies to protect us and maintain our national security is growing increasingly difficult. There is limited debate and discussion as to the necessity and proportionality of these powers. The Anderson Report which was championed by all sides of the Parliament was explicitly forbidden from discussing their proportionality. Rather, debate and argument centred on the limiting these powers via safeguarding. This places enormous pressure on the safeguards present in the IPA legislative framework to keep the use of these bulk powers to what is necessary and proportionate. The double-lock warrant authorisation system is foregrounded as the primary safeguard, alongside the oversight and supervision of the IPC and the exclusion of content data from bulk powers.

The remaining part of this chapter will set out the legislative framework which this process created. Beginning with a brief overview of the different bulk powers available under the legislation, the chapter outlines who and what the bulk powers can be applied to, before providing a brief overview of the safeguards present. This chapter aims to set up these key aspects of the legislative framework in summary in order to provide a foundation for later chapters analysing the harms and impacts of the bulk powers and the flaws present in the safeguards.

2.7 Powers under the Act

In terms of bulk surveillance practices under IPA 2016 the activities of the UK's security and intelligence agencies (SIAs) fall under four different powers: bulk interception, bulk acquisition, bulk equipment interference and bulk personal datasets. Interception can be described as a process where communications are collected in the course of transit, such that the content becomes available to someone other than the sender or recipient. The main focus of the examination of the intercepted communication must be overseas (foreign focused).[50] Bulk interception is the same basic process as this but typically involves the collecting of communications as they transit particular bearers (communication links).

Bulk acquisition gives the Secretary of State, on the application of the Head of an Agency and after approval by a judicial commissioner, the power to issue a bulk acquisition warrant. This warrant cannot apply to the content of communications but may require a

[50] Investigatory Powers Act 2016, s 129(2).

telecommunications operator to retain communications data and to disclose it to a person specified in the warrant. In contrast to Bulk Interception and Bulk Equipment Interference there is no requirement for bulk acquisition to be foreign-focused. The communications data of domestic communications such as phone calls and emails may be legitimately the intended focus for collection under the power. Additionally, unlike the other powers discussed here, data obtained through bulk acquisition can be aggregated in one place.

Bulk Equipment Interference covers a range of techniques involving interference with computers, the majority of which were previously known as computer network exploitation (CNE). While Equipment Interference (EI) includes more well-known techniques such as hacking or the implantation of software into endpoint devices or network infrastructure to retrieve intelligence, it can be as simple as copying data directly from a computer. EI is becoming increasingly useful to SIAs when compared with bulk interception practices. This is due to the fact that targets on which SIAs would use bulk interception have begun to use encryption as a means of bypassing this. EI renders any such peer to peer or end to end communication encryption moot by accessing the communications data at its origin, the device itself.

The fourth and final bulk power is the ability to retain and use Bulk Personal Datasets (BPD). Specific examples of BPDs disclosed include the passport register, the electoral register, the telephone directory and data about individuals with access to firearms. Broader categories disclosed include law enforcement/intelligence, travel, communications, finance, population, and commercial. BPDs generally contain basic biographical details on individuals that will correspond to the definition of "identifying data". While the specifics of these powers will be discussed in detail in chapters 4 and 5, what is clear from reviewing these powers is the sheer extent and breadth of action they confer on the SIAs who use them.

2.8 Who and What the UK Legislation Applies To

While the previous section outlines the array of available powers under the IPA, the scope of these powers remains ambiguous. The key to understanding the wide application of the IPA 2016 lies in the very broad definitions of communications and data contained within the Act. A communication is both "anything comprising speech, music, sounds, visual images or data of any description"[51] and signals which impart anything between persons, a person and an

[51] Investigatory Powers Act 2016, s 261 (2)(a).

object or between objects.[52] Data is defined as "any information (whether or not electronic)".[53] This very broad definition of data is then broken down into two types: identifying data and systems data. Identifying data includes:

(a) Data which may be used to identify, or assist in identifying, any person, apparatus, system or service;
(b) Data which may be used to identify, or assist identifying, any event; or
(c) Data which may be used to identify, or assist in identifying, the location of any person, event or thing.[54]

Systems data is then defined in the Act as meaning any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of the following:

(a) A postal service
(b) A telecommunication system (including any apparatus forming part of the system);
(c) Any telecommunications service provided by means of a telecommunication system;
(d) A relevant system (including any apparatus forming part of the system);
(e) Any service provided by means of a relevant system. A system is deemed relevant if any communications or other information are held on or by means of the system.[55]

In line with this broadness, a 'public telecommunications service' means any telecommunications service which is offered or provided to the public in any one or more parts of the UK.[56] A public telecommunications system means any telecommunication system located in the UK which provides a public telecommunications service or which consists of parts of any other telecommunication system by which a telecommunications service is provided. This leads to a telecommunications operator, to whom the majority of the legislation applies, being defined as a person who offers a telecommunication service to persons in the UK or controls or provides a telecommunications system which is wholly or partly in the UK or controlled from the UK.

The decision of the Act to rely on a broad definition of 'telecommunication operator' leads to a broad test to be applied whether a platform can be used to communicate between two

[52] Investigatory Powers Act 2016, s 261 (2)(b).
[53] Investigatory Powers Act 2016, s 263 (1).
[54] Investigatory Powers Act 2016, s 263 (2) (a-c).
[55] Investigatory Powers Act 2016, s 263 (4 – 5).
[56] Investigatory Powers Act 2016, s 261 (11).

people. This term not only includes network providers, but also the providers of a service that facilitates the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system. This is an intentionally broad definition as evidenced by the draft Codes of Practice: "Internet based services such as web-based email, messaging applications and cloud-based services" are covered by the Act.[57] Meaning that social media companies, while not explicitly mentioned, are within the scope of the Act. This is obvious for platforms with messaging systems as a primary function such as Facebook, Twitter, Whatsapp, Gab, and Telegram. It becomes less clear with platforms with messaging as a secondary or tertiary function. The primary function of YouTube for example is to upload and watch video content. There are three respects in which YouTube could be argued to be a communications platform. First, would uploading a video which informed your subscribers on some topic be considered communicating? Second, does commenting on a video count in the comments sections count as communicating with the video's creator or other users? Third, does privately messaging a user count as communication? The third is the most obvious to count as communication but the first and second are less certain. Addressing an audience of potentially thousands of anonymous users is difficult to square as communication from one person to another. Writing in a comment section could have the same logic as you aren't intending to communicate to one person in particular, however if a user replies to your comment and you respond then it more closely resembles peer to peer communication. YouTube would likely be considered within the scope of the Act. Storage sites like JustPasteIt, Dropbox and OneDrive are less certain. Uploading a document to your Dropbox is not considered communication between two people. It is unclear if uploading a document which is later accessed by another user should be considered a communication. It may come down to the content of the document, ie a letter addressed to the person who downloads it would be considered communication but it is impossible to know this prior to interception. Thus, any platform which could be used for communication, even if the platform wasn't designed for such a use, could be within the scope of the Act.

The fact that the majority of social media companies are located outside of the UK does not affect the scope of IPA 2016. If a company is outside the UK and provides a telecommunications service to people within the UK, or controls a telecommunication system in the UK, it is within the scope of the Act.[58] This is unsurprising considering that the

[57] Interception of Communications Code of Practice para 2.6.
[58] IPA 2016 s 261 (13).

majority of the powers within the Act, including the Bulk Surveillance Powers, expressly apply to non-UK persons and require them to do things outside the UK. Where powers are enforceable by injunction to persons outside the UK, such as in the case of interception warrants, the Act permits conflict with the law of another country to be taken into account.[59] This potential conflict is alleviated by acts such the Cloud Act in the USA as the majority of social media companies are American companies.[60] There is no such alleviation for platforms such as Telegram who move their base of operation from country to country often. The platform was founded in Russia but moved initially to Germany before moving again.[61] This is combined with how the company does not disclose where it rents its offices in order to "shelter the team from unnecessary influence"[62] and protect its users from governmental data requests. It is unclear how the jurisdiction of the IPA interacts with Telegram's method of forum shopping. They provide a telecommunications service to people within the UK so technically they are within reach but in practice it remains uncertain how an injunction can be served to such a mobile secretive company.

One of the main safeguards for each of the bulk powers is that they are required to be foreign focused, that is, they cannot be used to collect the communications data of those within the United Kingdom. This has been referred to as the British Islands safeguard.[63] However, this is an unclear provision considering the complexity of contemporary communication. An email which is sent from Reading and received in Birmingham may be routed through a Gmail server in California. It is unclear from the foreign focused safeguard whether such an email would be considered foreign focused. This foreign focus was defined as an 'external communication' under RIPA before being changed to 'overseas-related communication' under the IPA in an attempt to provide clarity.

Under RIPA an external communication is a 'communication sent or received outside the British Islands'. Under the IPA an overseas-related communication is either a communication sent by individuals who are outside the British Islands, or a communication received by

[59] Interception of Communications Code of Practice para 7.8.
[60] The Clarifying Lawful Overseas Use of Data (CLOUD) Act allows certain foreign governments, the UK is included in this, to enter bilateral agreements with the USA that will prequalify them to make foreign law-enforcement requests directly to American service providers. This bypasses the previous lengthy process of arranging a mutual legal assistance treaty (MLAT) with the US government directly.
[61] William Turton, "What isn't Telegram saying about its connections to the Kremlin?" *The Outline* (29 September 2017)
[62] John Thornhill. "Lunch with the FT: Pavel Durov". *Financial Times* (3 July 2015)
[63] Liberty v Secretary of State [2020] 1 W.L.R. 243 Para 49

individuals who are outside the British Islands.[64] While on the face of it this is a minor change, it eliminates the previous scenario under RIPA where an individual communicating with a server located outside the British Islands, for example when conducting a google search, would be considered an external communication. Thus, narrowing the scope of the IPA compared to RIPA. This change also clarifies the previous example as neither the sender in Reading nor the receiver in Birmingham are outside the British Islands and so their communications should not be interfered with through the bulk powers described under the IPA. The question remains as to how this works in practice. For example, it is unclear whether, when a bearer is tapped in a bulk interception operation, the technology collecting the data is able to discern between genuinely overseas-related communications and those which are merely being routed abroad. The alternative to this is that both types of communications are collected with the increased protection only being applied at a later stage.

The fact remains, however, that a person residing in the UK messaging a person residing in the USA will be considered an overseas-related communication. This situation is further complicated by social media where it is easy for the residence of social media users to change. For example, if I have a Facebook Messenger group chat with four friends, all of whom are in the UK, under the current definition our communications are protected from bulk interference. However, what happens when a fifth friend from France is added to the group chat? Under the current definition messages which are sent from that point on are received by an individual outside the British Islands. It's unclear whether only messages which are sent after the French addition are liable to be interfered with or if the group chat itself is considered an overseas-related communication and thus all messages are liable. Another complication comes from the inevitable occurrence that a member of the group chat goes on holiday abroad. While this is temporary, under the definition, messages in the chat then become overseas-related. As well as the questions raised by the French example, this raises a temporal aspect: are communications in the group chat considered overseas-related communications only for the duration of the holiday? There are two plausible answers to this question. The first is that the communications sent during this period are liable to be interfered with by bulk powers but that those sent prior and post the holiday are protected. The second is that both the communications sent during this period and those sent prior are

[64] IPA 2016 s136(3)

liable as they are saved within the group chat. Another scenario is raised by large quasi-anonymous platforms such as Telegram Channels or Discord groups, where it is nearly impossible to know if all the users are from the UK even in UK-centric groups. In these circumstances it seems impossible under the current definition for these users to avoid bulk interference with their communications.

There are also ambiguities to be found with what test authorities are using when conducting social media surveillance. Recently it was found through freedom of information requests that local authorities make extensive use of social media surveillance as part of their intelligence gathering and investigation tactics in areas such as council tax payments, children's services, benefits and monitoring protest and demonstrations.[65] This is done through both overt and covert monitoring. Overt monitoring is defined as the "casual (one-off) examination of public posts on social networks as part of investigations undertaken" and is permissible with no additional RIPA consideration. Covert monitoring is defined by the predecessor to the Investigatory Powers Commissioners Office, the Office of Surveillance Commissioners as "repetitive examination/monitoring of public posts as part of an investigation" and "must be subject to assessment and may be classed as Directed Surveillance as defined by RIPA."[66] 62.5% of local authorities use overt social media monitoring, and 31% use covert social media monitoring.[67] The distinction the local authorities are using between overt and covert seems to be based on the individual's privacy settings: "Where privacy settings are available but not applied data may be considered open source and an authorisation is not usually required."[68]

It isn't clear which of these tests is being applied by local authorities. The overt-covert distinction appears to be a test based on the number of times a social media post is examined by the local authority. While factoring in the individual's social media privacy setting appears to be a form of the reasonable expectation of privacy test. It is possible that the overt-covert distinction is simply a factor of their reasonable expectation of privacy test but then what accounts for the vastly differing levels of covert social media surveillance by different local authorities.

[65] Privacy International, 'When Local Authorities aren't your Friends' (2020) <https://privacyinternational.org/report/3584/when-local-authorities-arent-your-friends> accessed 06/06/2022
[66] ibid
[67] ibid
[68] Blaenau Gwent Country Borough Council Guidance

While this application of the reasonable expectation of privacy test to social media privacy settings may initially seem logical, it is in fact fraught with problems. First, it assumes that users have a reasonable knowledge of their available privacy settings and make the rational choice not to set them correctly. It may be difficult to find and change the setting you wish to change as in the case of the publicity of a Facebook friends list. A setting may be on by default without a user knowing that they can turn it off unless they are already privacy minded, such as Twitter's publishing of location data attached to a tweet. Second, as illustrated by the two previous examples, social media platforms differ widely and evolve rapidly and so do their privacy settings. Individuals may have multiple accounts on multiple platforms making it even more difficult to keep up with which privacy settings they should be updating in order to be considered private in the eyes of the UK authorities. This is compounded by the inclination of social media companies to make a user's posts and information as public as possible. This is not a nefarious plot by the social media companies but rather a consequence of their stated business aims, to maximise growth of audience and collection of data for marketing purposes.[69] It's clear that a reasonable expectation of privacy plays a formative role in the UK's authorities' approach to monitoring social media. However, it is difficult to say that, given these mitigating factors, it is reasonable to assume that the average user has conducted a thorough risk analysis of potential privacy harms from using social media. Madejski et al's study of 65 students found that despite their best efforts and intentions every single participant had incorrectly set their privacy settings and made public something which they didn't want to share.[70]

Returning to bulk surveillance, it is far more difficult to find official guidance on what social media data is considered public and what is considered private as it is conducted by more covert authorities such as GCHQ. It is likely considering how bulk surveillance operates in practice that both forms of data are intercepted in the process of bulk collection as they transit the tapped bearers. It is likely that the increased protection for private information only kicks in at the selection for examination stage, although it is again unclear as to how the automatic filtering system knows which information is valuable and should be kept for examination by analysts. This may be where the previously mentioned human officials assist in the filtering. This raises further questions however as these officials must access the data in order to decide

[69] Lilian Edwards and Lachlan Urquhart. "Privacy in public spaces: what expectations of privacy do we have in social media intelligence?." (2016) 24 International Journal of Law and Information Technology 279-310.
[70] Michelle Madejski, Maritza Lupe Johnson, and Steven Michael Bellovin. "The failure of online social network privacy settings." (2011). Columbia Academic Commons https://doi.org/10.7916/D8NG4ZJ1

whether it should be filtered before selection which in itself involves some violation of privacy. Returning again to the importance of the reasonable expectation of privacy test at work here, it cannot be reasonably expected of a social media user to consider that this series of interferences may occur to their data as they post their holiday photos on Facebook.

2.9 Review of Bulk Surveillance Powers

It is clear that the Bulk surveillance powers outlined above are far reaching and potentially very invasive. Two of these powers (bulk equipment interference and bulk personal datasets) have thus far been absent from the ECtHR's caselaw. This is unlikely to remain the case as these powers could be used on social media in future. Most social media use is done through applications on phones which can be hacked under bulk EI. The point made above by the SIAs that they are trying to catch up with the commercial sector likely refers to the commercial sector's practice of harvesting and selling advertising data. This is a major aspect of social media companies' business models and so it isn't too unlikely that social media data will end up in a bulk personal dataset either through direct purchase or indirect purchase or acquisition from advertising companies. It is likely that the use of these powers will form the basis of an ECHR case in future, especially considering the UK court's assertion in *Liberty v Secretary of State* that the ruling in *Big Brother Watch* on RIPA's convention incompatibility was not transferable to the IPA.[71] Overall it's clear that powers of such breadth and depth require significant safeguards in order to provide effective protection to individuals under the ECHR as implemented in the UK under the Human Rights Act (HRA). The following section outlines these safeguards in general rather than going through the safeguards for each power individually as, apart from bulk acquisition being able to be conducted within the UK, the same safeguards and authorisation apply for each power.

2.10 Safeguards and Supervision under the Investigatory Powers Act

Each of the powers outlined above has been shown to be broad in scope, far-reaching in effect, capable of collecting immense amounts of data, and operated covertly. In order to keep the use of these powers compatible with the Convention there must be correspondingly adequate and effective safeguards against abuse. This section first outlines the safeguards contained within the IPA regime to ascertain whether they fulfil the aforementioned criteria

[71] *Big Brother Watch and Others v. The United Kingdom* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018) para 140

of being adequate and effective safeguards against abuse. This begins by outlining the ex-ante safeguards primarily in the form of the so-called 'double-lock' warrant authorisation system, and the warrants themselves. The issues presented in this section provide the basis for chapter 8 on judicial authorisation.[72] Next, the section outlines the safeguards surrounding the ex post safeguards, primarily in the form of the Investigatory Powers Tribunal, and the Annual Reporting by the Investigatory Powers Commissioners Office. The issues present in this section form the basis for a subsequent chapter on the lack of procedural justice present in the proceedings of the IPT.[73] Finally, this chapter outlines the comparative lack of safeguards during the operation of bulk surveillance. This forms the crux of this thesis. The ex ante and ex post safeguards are flawed and in need of further reform, but an even greater issue is the lack of safeguards in place *during* the operation of the surveillance regime.

2.11 Supervision and Safeguards Prior to Operation (Ex ante)

2.11.1 Judicial Authorisation

Before a bulk powers warrant can be issued, the Secretary of State's decision to issue it must be approved by a Judicial Commissioner.[74] The Judicial Commissioner will review the Home Secretary's conclusions as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved.[75] The Judicial Commissioner will also review the Home Secretary's conclusion as to whether each of the operational purposes specified on the warrant is a purpose for which the use of said power is, or may be, necessary.[76] This judicial authorisation might be argued to be a positive element of the Act, and an important safeguard. Given that any investigatory powers warrant will necessarily engage human rights, the judiciary is best positioned to decide their compatibility with the ECHR. This system is referred to as the 'double-lock' safeguard in the various codes of practices pertaining to the Investigatory Powers Act. However, the overall effectiveness of this safeguard needs to be examined in more detail.

Debate during the drafting of the IPA centred on two arguments: institutional competence and democratic accountability. For example, Lord Carlile, a former reviewer of terrorism legislation, argued that in principle the issue of warrants should be for Ministers alone. This

[72] See chapter 8 on 'Authorisation and Examination Mechanisms under the IPA 2016'
[73] See chapter 9 on 'Review and Oversight in the Investigatory Powers Regime'
[74] IPA 2016 s 140
[75] Ibid s 140(1)
[76] Ibid para 4.13

is both on the grounds of institutional competence - Ministers have material information and expertise which the judiciary does not - and in terms of democratic accountability, as ministers are accountable to Parliament and in turn the electorate.[77] In contrast, others like the Bingham Centre argued that the Act doesn't go far enough to ensure judicial scrutiny of decisions to issue warrants, that the Secretary of State should apply for the warrant from the JC, wherein democratic accountability would be derived from the Secretary applying for a warrant.[78] Anderson, another former reviewer of terrorism legislation, agreed with the Bingham Centre on this ground but only for the authorisation of targeted warrants. Bulk, thematic, and any warrants pertaining to foreign policy or national security were to be subject to the original double-lock system.[79]

Examination of this safeguard raises a number of issues. First, there is the question of the appropriate role of the judiciary in this context, given the need to balance the separation of powers, the executive's prerogative to protect national security, and the need to protect human rights in line with the HRA 1998. Next there are questions about the appropriate standard of review to be applied by the JCs and the appropriate level of deference that should be given to the Secretary of State in the double-lock context. Finally, there are institutional factors to be considered such as appointment methods and terms and the remit of the IPC. These issues will be examined in greater detail in a later chapter.[80]

2.11.2 Warrants – Bulk and Thematic

The IPA 2016 replaces RIPA's system for bulk interception warrants. A bulk interception warrant can be issued if preconditions A and B are met. Precondition A concerns the main purpose of the warrant and precondition B concerns the specifics of the interception. For Condition A to be fulfilled the main purpose of the warrant must be one or more of the following;

(a) The interception of overseas-related communications.
(b) The obtaining of secondary data from such communications[81]

Overseas-related communications are defined in the Act as communications sent or received by individuals who are outside the British Islands. Precondition B is that the warrant

[77] Lord Carlile of Berriew CBE QC – written evidence (IPB0017)
[78] Bingham Centre for the Rule of Law – written evidence (IPB0055)
[79] David Anderson QC – supplementary written evidence (IPB0152)
[80] See chapter 8 on "Authorisation and Examination Mechanisms under the IPA 2016"
[81] Investigatory Powers Act 2016 s 136(2) (a-b)

authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following activities:

(a) The interception, in the course of their transmission by means of a telecommunication system, of communications described in the warrant.
(b) The obtaining of secondary data from communications transmitted by means of such a system and described in the warrant
(c) The selection for examination, in any manner described in the warrant, of intercepted content or secondary data obtaining under the warrant.
(d) The disclosure, in any manner described in the warrant, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.[82]

The warrant also authorises any conduct which is necessary to undertake what is expressly authorised by the warrant. This includes the interception of communications not described in the warrant, the obtaining of secondary data from such communications and obtaining related systems data from any telecommunications operator.[83]

The IPA states that the Secretary of State may issue a bulk interception warrant upon application from the Head of an intelligence agency. The IPCO provides a list of those who qualify as a head of an intelligence agency: "the Director General MI5, the Chief of SIS, the Director of GCHQ, the Director General of the NCA (on behalf of the NCA or police forces for serious crime), the Metropolitan Police Commissioner (for counter terrorism), the Chief Constable of the Police Service of Northern Ireland, the Chief Constable of Police Scotland, HMRC Commissioners and the Chief of Defence Intelligence."[84] This interception must be necessary for one or more of the following;

(a) In the interests of national security
(b) To prevent or detect serious crime
(c) Safeguarding the economic well-being of the United Kingdom

[82] Investigatory Powers Act 2016 136(4) (a-d)
[83] Ibid 136(5)(a)
[84] Investigatory Powers Commissioner's Office, *Annual Report of the Investigatory Powers Commissioner*, (2017) p 40

(d) In circumstances equivalent to those in which the Secretary of State would issue a serious crime warrant for implementing an international mutual assistance agreement.[85]

Issuing an interception warrant for any other reason would be unlawful. Additionally, the Secretary of State may not issue a warrant unless they believe that the conduct authorised by the warrant is proportionate to what is sought to be achieved. In 2017 a total of 3,535 warrants were issued, a 17.5% increase over 2016. On 31 December 2017 there were 1,974 warrants in force, a 23.3% increase on the number extant at the end of 2016. 21 of these warrants were issued under the bulk provisions. This speaks to several possibilities. Either bulk surveillance warrants are not utilised often, or the volume of data garnered from these 21 warrants is sufficient for the purposes of the intelligence agencies.

The IPA also introduces thematic warrants. Section 17(2) provides additional permissions to apply for interception warrants or targeted examination warrants. These may relate to:

(a) A group of persons who share a common purpose or who carry on, or may carry on a particular activity;
(b) More than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation; or
(c) Testing or training activities.[86]

Thematic warrants must include certain additional details depending on the subject matter of the warrant. The code of practice gives the example of a thematic warrant that relates to a group that shares a common purpose. It must include a description of that purpose as well as the name or description of as many of the persons who constitute that group as it is reasonably practicable to name or describe. These descriptions must include as many of the persons, organisations or sets of premises as is reasonably practicable and must be as granular as reasonably practicable in order to sufficiently enable proper assessment of the proportionality and intrusion involved in the interception.

It may not always be reasonably practicable to include descriptions of every person, organisation and premises involved in the operation. Thus, thematic warrants are divided into two types, those where it is reasonable to include additional details and those where it isn't.

[85] ibid
[86] IPA 2016 s17(2)

The code of practice gives an example of each and in doing so provides an indication of the variance in the size of operation covered by thematic warrants:

> **Example of warrant where it is reasonably practicable to individually name those falling within the subject matter of the warrant:** An intercepting authority wishes to intercept the communications of three people for the purposes of an investigations into human trafficking. The agency apples for a warrant in relation to "more than one person for the purpose of operation X" and those persons are known to be 'Mr A', 'Mr B' and 'Mrs C'. As it is reasonably practicable to do so their names must be included in the warrant at the point of issuing. Once issued the warrant authorises the interception of the communications of 'Mr A', 'Mr B' and 'Mrs C' which are identified by factors specified in the warrant. Further factors or further names or descriptions may be added by modification … if the agency wishes to undertake further activity.
>
> **Example of warrant where it is <u>not</u> reasonably practicable to specifically name or describe those falling within the subject-matter of the warrant:** An intercepting authority wishes to identify persons accessing terrorist material online. The authority seeks a thematic warrant in relation to more than one person for the purpose of a single investigation, with the subject-matter of the warrant being "persons accessing the terrorist website 'X'". In such a case, it may not be reasonably practicable to name or describe those persons any further than by a description which is based on their use of website 'X'. Once issued the subject-matter of this warrant is any person known to be accessing the terrorist website 'X' and the interception of the communications of any person falling within that description is lawful. There is no requirement to modify the warrant in accordance with section 34 to add names or description of person accessing the website.[87]

The gap between these two types of thematic warrants is huge. Example A falls neatly into the flexibility argument for thematic warrants. It would not be reasonable to expect each of the individuals to be subject to a separate targeted interception warrant and may actively hinder the operation in question. If through intercepting these three individuals' messages they found a 'Mr or Mrs D' who had an active role in the human trafficking operation they could modify the existing warrant to include them without slowing the investigation down.

[87] Interception of Communications Draft Code of Practice s 5.14

Example A is not comparable to Example B. In A, the number of people covered is limited initially to three with the possibility of adding more if necessary. In B, there is no set limit of the number of individuals who could potentially have their communications intercepted at the beginning and no upper limit on how many could by the end. These are qualitatively different forms of surveillance. In A there is suspicion of three persons of interest which justifies the warrant, in B there is simply a website URL which contains terrorist material. Where A can reasonably be described as a thematic warrant in that it is the combination of multiple targeted warrants designed for expediency's sake, B is something more akin to a more targeted form of bulk surveillance. In the A case if the SIA wished to add another person to the warrant they would need to be authorised by a senior official in one of the warrant granting departments and notified to the JCs afterwards. In the B case no such authorisation is required. This points to a larger issue where each of these situations require different approaches and safeguards.

2.12 Supervision and Safeguards Post Operation (Ex-Poste)

This leads us to the two ex post safeguards in the UK system of surveillance: the Investigatory Powers Tribunal (IPT), and the annual review conducted by the Investigatory Powers Commissioner's Office (IPCO). This section aims to outline each of these safeguards fully as part of this chapter's overall evaluation of the UK surveillance regime under the Investigatory Powers Act 2016.

2.12.1 The Investigatory Powers Tribunal; An Overview

The Investigatory Powers Tribunal was set up under RIPA 2000 to ensure the UK meets its obligations under Article 13 of the ECHR to provide an effective remedy.[88] It is an independent judicial body which provides a right of redress for anyone who believes they have been subject to unlawful surveillance in the UK.[89] The Tribunal is also the appropriate forum to consider complaints about the conduct of the UK intelligence community.[90] The Tribunal has jurisdiction across the UK and there are no costs associated with making a complaint to it.[91]

[88] The Investigatory Powers Tribunal, General Overview and Background https://www.ipt-uk.com/content.asp?id=10
[89] Regulation of Investigatory Powers Act 2000 s 65(2) (a-d)
[90] Ibid s 65(4)(a-b)
[91] The Investigatory Powers Tribunal, Frequently Asked Questions https://www.ipt-uk.com/content.asp?id=24

The question which remains is whether the IPT in its current form is an effective remedy for those subjected to surveillance, either bulk or targeted. This question has been put before the ECtHR in *Kennedy* and *Big Brother Watch*. In both it was found to be an effective remedy in that its limitations were justified by the context in which it operates.[92] The combination of the pursuit of national security or preventing serious crime with the covert nature of surveillance justified the restrictions on equality of arms,[93] disclosure of relevant evidence,[94] and provision of reasons.[95] Additionally the IPT has been subject to reform since its establishment in RIPA 2000 which this section will attempt to outline.

It is important to note that the IPT is not a court of law, or even an inferior court of law, nor is it a court of record. It has an investigatory, not adversarial, function in respect of certain complaints made to it. The Tribunal's investigatory function can be viewed as a safeguard as the adversarial function of more traditional courts is not suited to the context of secrecy.[96] In order to protect the secrecy of the investigations and operations it examines, the Tribunal is subject to significant restrictions as to the level of information and nature of determinations it can disclose.[97] It is for the applicant to argue in favour of disclosure but this is an incredibly difficult task.

In terms of the organisation of the IPT, only the President is required to hold or have held judicial office[98] and there is no statutory requirement that complaints are adjudicated by the President.[99] The Tribunal is required to comply with rules which are made by the Secretary of State rather than itself or the Civil Procedure Rules Committee.[100] The Secretary of State is effectively a party to many of the matters that the Tribunal considers.[101] This raises questions about the independence of the Tribunal, as the executive sets the parameters for the examination of its own decisions. While in practice this may not impact how the Tribunal rules it does create the perception of bias and may undermine public confidence in the Tribunal as a check on the executive's use of power in a national security context.

---

[92] *Big Brother Watch and Others v. The United Kingdom,* App nos. 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018), para 318
[93] *Kennedy v United Kingdom* (2011) 52 EHRR 4 para 184
[94] Ibid para 187
[95] Ibid para 189
[96] Alisdair Gillespie and Siobhan Weare, *The English Legal System* (OUP 2019) p 233
[97] Investigatory Powers Tribunal Rules 2000 s (6)(1-7)
[98] RIPA 2000 Sch.3 para 2
[99] Ibid para 1
[100] RIPA 2000 (69)(1 – 2)
[101] ibid

Unlike other tribunals, the IPT is not open to the public. It was created by Part IV of RIPA. The Tribunal has been described as "being different from all others in that its concern is with security. For this reason it must remain separate from the rest and ought not to have any relationship with other tribunals."[102] While it is true that the IPT is concerned with security, the implications of this are open to debate. There is a tension present here in that while courts are prima facie public bodies and thus should sit in public and pronounce decisions publicly, the investigatory powers at play here are sensitive enough that the Government would not wish them to be discussed in public for fear that such publicity could assist those who the powers are used against.[103] The detailed use of investigatory powers will often be kept secret, even in criminal trials, through a process called Public Interest Immunity.[104]

Under the HRA, someone who believes that such powers are being used inappropriately against them has the right to take action against the authorities. The IPT is this action.[105] In fact, the IPT is their only available action[106] as it is seen as the sole appropriate tribunal to consider measures of surveillance.[107] This position was based partly in the fact that the decisions of the IPT are not ordinarily subject to an appeal.[108] Prior to May 2019, the IPT was not subject to review by higher courts. Section 67(8) of RIPA states that:

> Except to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court.

This ouster clause was upheld by the UK Divisional Court in *R (Privacy International) v Investigatory Powers Tribunal* as the Court found that the IPT performs the sort of supervisory function normally performed by the High Court, in cases which the ordinary court system cannot handle due to the fact that they involve "highly sensitive material and activities which need to be kept secret in the public interest".[109] While this judgment has

[102] Andrew Leggatt, *Tribunals for Users: One System, One Service* (HMSO 2001) para 3.11.
[103] Alisdair Gillespie and Siobhan Weare, *The English Legal System* (7th edn. OUP 2019)
[104] Andrew Ashworth and Mike Redmayne, *The Criminal Process* (4th edn, OUP 2010).
[105] HRA 1998, s 7
[106] RIPA 2000, s 65(2), upheld in *R (on the application of A) v B* [2009] UKSC 12.
[107] IPA 2016 s 243
[108] ibid
[109] *R (Privacy International) v Investigatory Powers Tribunal* [2017] EWHC 114 (Admin) para 41

significant implications for the rule of law,[110] the provisions governing the Tribunal were expanded in IPA 2016 to provide a new right of appeal from decisions and determinations of the Tribunal in circumstances where there is a point of law that raises an important point of principle or practice, or where there is some other compelling reason for allowing an appeal.[111]

While the rules of the tribunal are set out in the Investigatory Powers Tribunal Rules 2018, RIPA itself states that the IPT shall, subject to rules made by the Secretary of State under section 69(1), determine its own procedure in respect of complaints. This is understood as meaning that the IPT can issue its own rules but also that it may alter them depending on the circumstances.[112] This is most easily explained as being a form of discretion conferred on the Secretary of State by RIPA.[113] The rule-making power of the Home Secretary is a wide one, as they may make rules regulating the exercise by the Tribunal of the jurisdiction conferred on them by section 65 of RIPA. Although particular types of provision potentially covered by the exercise of power to make rules are set out, the particular topics singled out for special mention are "without prejudice to the generality" of the discretion of the Secretary of State.[114] The use of this discretion by the Home Secretary took the form of the original, and updated, IPT Rules which place a number of duties on the Tribunal including a general duty to restrict disclosure of information.[115]

While this is a large amount of influence for the executive to hold over the IPT, the Tribunal has struck down one section of the rules which required it to conduct their proceedings, including oral hearings, in private.[116] Using its position as the sole arbiter of claims under the HRA the IPT took the position that, where the rules are incompatible with the ECHR, the Tribunal reserves the right to be the ultimate arbitrator of its own procedure.[117] The blanket nature of the rule to conduct proceedings in private was "fatal to its validity" as the Tribunal found that the broadness of such a rule went beyond what was authorised by section 69 of RIPA.[118] Thus the Tribunal concluded that rule 9(6) is ultra vires section 69 RIPA and did not

[110] Scott, P. F. 'Ouster clauses and national security: judicial review of the investigatory powers tribunal' (2017) 17 Public Law 355-362
[111] Investigatory Powers Act 2016 s(242)
[112] Alisdair Gillespie and Siobhan Weare, *The English Legal System* (7th edn. OUP 2019)
[113] In the Matter of Applications Nos IPT/01/62 and IPT /01/77 (2003) Para 36
[114] RIPA 2000 s 69(2)
[115] IPT Rules, r 6
[116] Ibid, r 9
[117] Alisdair Gillespie and Siobhan Weare, *The English Legal System* (7th edn. OUP 2019) p 233
[118] In the Matter of Applications Nos IPT/01/62 and IPT /01/77 (2003) Para 167

bind the Tribunal. The complainants in that case then contended that the Tribunal is entitled and bound to exercise its procedural power under section 68(1) of RIPA so as to achieve compatibility with Convention rights, as the relevant rules are ultra vires and there are no provisions in RIPA that require them to do otherwise.[119] However, the Tribunal concluded that it only has discretion under section 68(1) in respect of three relevant areas of procedure:

- Whether to hold an oral hearing with all parties present;
- Whether to hold the hearing in public; and
- Whether to publish detailed reasons for their rulings on pure questions of law concerning procedure and practice.[120]

It further added that the Secretary of State could remove this discretion by amending the rules on said relevant areas. So then the ability of the Tribunal to be the sole arbiter of its own procedure is extensively limited by the discretion of the executive.[121] Add to this the reform in the IPA which removed the ouster clause by allowing for appeals from the IPT to a higher court. Interestingly, the removal of the ouster clause has removed the ability of the IPT to claim to be the sole arbiter of its procedure. It is unclear how this interacts with their ability to set their own rules under RIPA as the IPT used their position as sole arbiter in order to defy the rule that it had to hold cases in secret.

This section has shown how the IPT has developed in the 20 years since it was established. Arguably these reforms have been an improvement, such as the removal of the obligation to sit in secret and the removal of the ouster clause. Nonetheless, the operation of the IPT raises a number of issues such as the lack of transparency surrounding its judgments. The Tribunal is still limited in the amount of substantive and procedural justice it can provide claimants and the Tribunal could alleviate some of these issues through the implementation of reforms derived from other measures which deal with sensitive materials, namely Public Interest Immunity and Special Advocates. These issues will be returned to in chapter 6.[122]

2.11.2 Annual Review, Auditing and Inspection by the Investigatory Powers Commissioner's Office

[119] Ibid para 193
[120] Ibid para 195
[121] Ibid para 173
[122] See Chapter 9 on the "Review and Oversight in the Investigatory Powers Regime"

The IPCO inspections of the use of investigatory powers are done with three objectives in mind: (a) to ensure that compliant authorisations have been given, (b) to ensure that legal requirements (such as necessity and proportionality) have been met, and (c) that standards of good practice are maintained. The IPCO emphasises that one size of inspection does not fit all, that the IPCO is flexible in their approach to inspection to ensure the demands they make on public authorities are proportionate but allow them the required access. These inspections and auditing processes will be returned to in greater detail in chapter 9. Another safeguard, in line with the inspections and auditing, is the annual review of the use of Investigatory Powers conducted by the Investigatory Powers Commissioner. This is a general oversight mechanism. The IPC must, as soon as reasonably practicable after the end of each calendar year, make a report to the Prime Minister about the carrying out of the functions of the JCs.[123] As set out in the legislation these reports must include:

(a) statistics on the use of the investigatory powers which are subject to review by the IPC (including the number of warrants or authorisations issued, given, considered or approved during the year),
(b) information about the results of such use (including its impact),
(c) information about the operation of the safeguards conferred by this Act in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic information,
(d) information about the following kinds of warrants issued, considered or approved during the year –
    i. targeted interception warrants or targeted examination warrants of the kind referred to in section 17(2),
    ii. targeted equipment interference warrants relating to matters within paragraph (b), (c), (e), (f), (g) or (h) of section 101(1), and
    iii. targeted examination warrants under Part 5 relating to matters within any of the paragraphs (b) to (e) of section 101(2),
(e) information about the operational purposes specified during the year in warrants issued under Part 6 or 7,
(f) the information on errors required by virtue of section 231(8),
(g) information about the work of the Technology Advisory Panel,

[123] IPA s 234 (1)

(h) information about the funding, staffing and other resources of the JCs, and

(i) details of public engagements undertaken by the JCs or their staff.[124]

Upon receipt of this report, the Prime Minister must publish it and present it to Parliament. Although the PM may, after consultation with the IPC, exclude any part of the report from publication if the PM thinks that such publication would be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the UK or the continued discharge of the functions of any public authority whose activities are subject to review by the IPC. As indicated above, the IPCO reports as described in section 234 are very detailed and useful tools for promoting the transparency of the surveillance regime under the IPA. For example, they have already been used to show the JC's authorisation rates. However, the problem with this safeguard is that while they are transparent, transparency can only go so far in this field as a safeguard.[125]

2.12 Supervision and Safeguards during operation

The previous sections have described in detail the ex ante and ex post safeguards surrounding the bulk surveillance regime under the IPA 2016. These safeguards contain a number of serious issues which will be discussed further in the chapters 8 and 9. By contrast, the issue with the supervision and safeguards *during* operation is that there are not many safeguards at all. Additionally, the oversight and safeguards which do exist are limited by the fact that they are implemented as part of the ex ante stage.

2.12.1 Oversight

As per the Investigatory Powers Act 2016, there is limited oversight of GCHQ as it collects massive amounts of data through the process of bulk interception. Under Chapter 1 of Part 6 of the Act a Bulk Interception warrant may only be issued to the intelligence services and must meet two conditions. The first is that its main purpose must be limited to the interception of overseas-related communications and/or the obtaining of metadata from such communications. Overseas-related communications are defined at section 136(3) of the Act as those that are sent or received by individuals outside the British Islands.

The second condition is that the warrant authorises or requires the person to whom it is addressed to do one or more of the following: to intercept communications described in the

[124] IPA s 234 (2) (a-i)

[125] See chapter 9 on 'Review and Oversight in the Investigatory Powers Regime'

warrant, to obtain secondary data from such communications, to select for examination the intercepted content or secondary data, or the disclosure of anything obtained under the warrant. A bulk interception warrant must also set out specified operational purposes, and no intercepted content or secondary data may be selected for examination unless doing so is necessary for one or more of the operational purposes specified on the warrant. As discussed above said interception must be necessary to achieve one of the legitimate aims outlined above.

So long as the warrant meets the above requirements it does not need to limit itself to a named or described person, organisation or set of premises in carrying out the interception. Neither does Chapter 1 of Part 6 impose a limit on the number of communications which may be intercepted. The code of practice on bulk interception gives the example that "if the requirements of this chapter are met then the interception of all communications transmitted on a particular route or cable, or carried by a particular telecommunications operator, could, in principle, be lawfully authorised". As will be discussed further in chapter 4[126], the intrinsic nature of bulk interception means that there is limited opportunity for effective safeguards at the point of interception. The key opportunity, in terms of safeguards, is instead at the later stage when intercepted materials are examined.

2.12.2 Operational Purposes

The Draft Code of Practice on Communication Interception describes additional safeguards for the examination of material collected through bulk interception. These are derived from section 152 of the IPA. The first of these is that selection for examination may only take place for one or more of the operational purposes specified on the bulk interception warrant. Terminologically this description is slightly muddled by the overuse of the word 'purpose'. Throughout the Code of Practice for example, refers to:

"whether the application is necessary for one or more of the permitted statutory purposes (in the interests of national security, for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security)"[127]

[126] See Chapter 4 "Understanding the Harms of Bulk Interception"
[127] Interception of Communications Draft Code of Practice para 6.19

For clarity, the operational purposes discussed in this chapter are to be distinguished from the statutory purposes set out in part A of the warrant section such as national security, or the prevention of serious crime. Operational purposes are necessarily narrower than statutory purposes as they describe what exactly the data selected for examination is going to be used for.

The Code of Practice provides two examples of operational purposes:

"to establish links between known subjects of interest, improving understanding of their behaviour and the connections they are making or the multiple communications methods they may be using;"

And:

"to search for traces of activity by individuals who may not yet be known but who surface in the course of an investigation, or to identify patterns of activity that might indicate a threat to the United Kingdom."[128]

These are still quite broad examples. They might have been written as such in order to provide a general example of what an operational purpose could be. The requirement to be an operational purpose could equally apply to narrower descriptions such as to detect the activity of a proscribed terrorist group like ISIS.

In order for an operational purpose to be specified on a bulk warrant it must relate to the statutory purposes set out in said warrant; such as national security, prevention of serious crime etc. The Secretary of State may not approve the addition of an operational purpose to the central list unless they are satisfied that the operational purpose is more detailed and specific than the relevant statutory grounds. Operational purposes must then have a clear requirement and contain sufficient detail in order to satisfy the Home Secretary that intercepted material may only be selected for examination for specific reasons. It is possible to alter a bulk warrant to add a new operational purpose but this is subject to a strict approval process. The central list must also be reviewed annually by the Prime Minister and shared every three months with the Intelligence and Security Committee.

[128] Home Office, *Interception of Communications Code of Practice* (2018) para 6.4

It is left open to speculation what this centralised list looks like. It is not made public due to security concerns. However, it seems likely that the operational purposes on this list are of a general nature otherwise the list would be exhaustively long and new operational purposes would have to be added with every warrant. As stated above, the test is for the operational purpose to be more detailed than a statutory ground, for it to have a clear requirement and be specific enough that intercepted material can only be selected for examination for those specific reasons. Returning to the example above, the detection of a specific terrorist group such as ISIS is likely an operational purpose on the centralised list. It is narrower than its corresponding statutory ground, it has a clear requirement, and doesn't allow material that doesn't pertain to potential ISIS activity to be selected for examination. On the other hand, it does allow such material to be collected, and comprises quite a broad net for collection as it would likely allow the interception of all messages between the UK and any country in which ISIS has been active. This again shifts the weight of safeguards from collection to selection for examination as the safeguards do not effectively kick in until the selection for examination stage.

This lack of clarity on the extent of operational purposes is explained away by the intelligence services' need to retain their operational agility in the face of developing and changing threats. The covert nature of these operations, while unmentioned, certainly plays a role in the decision not to publish these operational purposes. However, under section 142 of the Act the Heads of the intelligence services must maintain a central list of all the operational purposes which they consider are purposes for which intercepted data may be examined under. This central list acts as the master list as an operational purpose may not be specified on a bulk warrant unless it is specified on the central list. Before an operational purpose may be added to that list, it must be approved by the Secretary of State. In the case of bulk warrants, in practice, said new operational purpose must be approved by both the Home Secretary and the Foreign Secretary. It is unclear what the benefit of ascribing this function to the executive is, over the Chief Justice or Investigatory Powers Commissioner. If the purpose of the operational purposes safeguard is to narrow the permitted usage of bulk powers, entrusting the executive with the power to add an ever-increasing amount of purposes to the list may undermine this safeguard.

No data can be selected for examination other than for the specified operational purposes. Here the draft code of practice advises that automated systems should, where possible, be used to filter the selection for examination. However, it also acknowledges that a limited

number of officials should be given access to the system during this process of filtering, processing and selection in order to ascertain, for example, system health. This access must be necessary to both the operational purposes of the warrant and to the statutory grounds outlined in sections 138(1)(b) and 138(2). This access is also subject to review by the Investigatory Powers Commissioner. This provides a tension with the justification that bulk surveillance powers are less intrusive on individual's privacy because the data collected is subject to algorithmic filtering rather than human eyes. If individuals are allowed to view this data prior to filtering and without the safeguards present at the selection for examination step then this argument of algorithmic surveillance being less intrusive is undermined considerably.

The purpose of the operational purposes safeguards is ostensibly to provide a tougher necessity standard for the examination of collected material than is present at the initial collection stage. Since the weight of the safeguards in the IPA system falls squarely on the selection for examination stage, such safeguards must be sufficiently stringent. In the case of operational purposes, they must be sufficiently narrow to provide this level of safeguard, in order to sufficiently limit the amount of collected data which can be examined. The examples given by the Code of Practice above are not sufficiently narrow to satisfy this test. In their current form they are general descriptions of what bulk surveillance might be used for. For example, narrowing these examples to members of specific proscribed groups would provide a stricter safeguard. This way, the approval process to add new operational purposes would act as filtering method as to whether it is necessary to subject certain groups to bulk surveillance, rather than the current system which seemingly allows for the surveillance of any individuals who may not yet be known but might indicate a threat to the United Kingdom. Given the weight that the current system places on examination safeguards, the operational purposes safeguard does not appear to be implemented with sufficient rigour at present.

2.13 Applying the same safeguards to qualitatively different powers

Taken as a whole the four bulk surveillance powers outlined in the IPA 2016 confer incredible surveillance capabilities on the SIAs authorised to use them. Bulk interception allows them to collect any communication which transits a particular bearer. Given the sheer volume of communications which are transmitted through the internet in a given moment, the ability to tap just one of these bearers for a period of months would result in the collection of

millions of communications. Bulk acquisition allows them to require telecommunication companies to retain and disclose a large volume of communications. The amount of information collected becomes stark if one thinks of a social media company such as Facebook disclosing even a fraction of their retained data. It is equally stark when it comes to the telecoms companies like BT or Virgin who are within the scope of the power too due to it lacking a foreign focus safeguard. It is unclear from reading the legislation exactly how bulk equipment interference works in practice but in order to interfere with devices on a bulk scale the SIAs would likely have to install some form of malware on the devices in question, perhaps hidden in an app. Importantly, bulk EI bypasses the precautions an individual may take in order to avoid the first two powers as it bypasses peer to peer encryption. Finally, bulk personal datasets resemble in their scope more stereotypical views of surveillance wherein information which individuals must give away at various instances in order to participate in society are collated in massive databases which can be accessed upon request. These are clearly broad powers which are in need of correspondingly strict safeguards to be considered compatible with Article 8 ECHR, under the end-to-end safeguards test as per the grand chamber judgment of *Big Brother Watch*.[129]

While these powers are uniformly broad, they are qualitatively different forms of surveillance. Each has a different approach to obtaining data. Interception takes the data mid-flight, acquisition takes from the companies who hold the data, equipment interference takes from the root of the communication, the device itself, and bulk personal datasets collate available data into large searchable datasets. Each has a differing expectation of privacy associated with it on the part of the individual. The reasonable expectation of privacy when sending an email to a friend abroad is different than simply using a telecommunication service. Likewise, the expectation of privacy of owning a smartphone and downloading a government application is different to the expectation when giving your personal information to a bank when opening an account. Additionally, as seen in chapter 1 the technology behind each is also qualitatively different.

With this in mind it becomes clear that the legislation's application of the same set of safeguards to each power is inadequate. The only difference in said application is that the foreign focus safeguard is not applied to bulk acquisition. This is likely due to how the power would be unable to function properly if it was restricted to foreign companies which the UK

[129] See Chapter 6 on "Bulk Interception Caselaw of the ECHR"

government doesn't have jurisdiction over. Still, the absence of one of the most important safeguards on bulk surveillance in bulk acquisition necessitates the introduction of stringent safeguards to account for it. This highlights how specialised safeguards for each power should be introduced going forward.

While this is the most egregious example the safeguards applicable to each of the other powers could be better suited to the specific power. Currently, the system seems to be a set of safeguards for bulk interception which have been crudely stretched to cover the other powers. For example, in each the weight of the safeguards is placed on the selection for examination stage, as this is seen to be the real interference with the individual's privacy. The collection en-masse and the automatic filtering are seen as lesser interferences as they are, in a way, anonymous. However, how does this logic interact with equipment interference? Interfering with an individual's computer or smartphone which contains countless incidents of identifying and personal data, especially if the intent is to bypass encryption, is a far greater interference on an individual than collecting millions of messages as they cross a specific bearer. This interference is even more severe considering the fact that these devices are personal property. Bulk equipment interference thus requires a set of safeguards which places weight on the collection step rather than the selection for examination step.

2.14 Conclusion

This chapter has shown how the UK legislation has provided SIAs with updated powers that are fit for the modern age and contemporary forms of communication. However, the implementation of human rights safeguards has failed to keep pace with the creation and the practical realities of these new powers, in at least three respects. First, the definition of key terms, and therefore the scope of the powers) are an awkward fit for modern forms of communication, leaving the ambit of the powers unclear. Second, as will be covered further in chapter 5, there are significant difference between the different powers conferred, yet the safeguards largely apply homogenously, meaning that they are ill-suited to some of the powers in question.[130] Third, the safeguards largely apply ex-ante and ex-post, with insufficient oversight at the crucial selection for examination stage.

Beginning with the ex-ante safeguards. The so called double-lock system is not as secure a process as the name suggests. The 'double-lock' comes from how an application for a

[130] See chapter 5 on 'Understanding Bulk Powers as Qualitatively Different from Each Other'

surveillance warrant must be approved by the Secretary of State before being approved by a Judicial Commissioner. Thus, the discretion of the executive is checked by judicial authority. However, it is unclear what level of scrutiny the Judicial Commissioner operates under on a given application. Within the Act itself the JC is limited to judicial review, which is specified to mean only assessing the procedural aspects of the application. However, these warrants interfere with Article 8 ECHR. The UK courts have adopted a proportionality approach in their judicial review of decisions affecting ECHR rights. Thus, the JCs have the ability to assess the proportionality of these measures outlined in the warrant application but it is unclear whether they do so or are willing to do so. This question forms the basis of chapter 8 on authorisation mechanisms within the IPA, which also addresses questions of appropriate deference and the appropriate role of the judiciary in this context.

In terms of ex post safeguards, this chapter covered two institutions: the Investigatory Powers Tribunal, and the annual review, auditing and inspections by the Investigatory Powers Commission Office. The chapter first showed how the IPT has developed over the 20 years since its establishment, highlighting how the Tribunal has been subject to reforms such as the removal of the obligation to sit in secret and the ouster clause. However, this chapter also outlined briefly issues with the IPT, namely the Tribunal is limited in the amount of substantive and procedural justice it can provide to claimants. The chapter next outlined the safeguard provided by the IPCO. Like many of the IPA safeguards, this struggles with the inherent covert nature of surveillance. These issues will be returned to in Chapter 9, which evaluates the IPT as a domestic remedy as part of a larger analysis of review and oversight mechanisms in the IPA and the efficacy of the IPCO's inspections, auditing, and reporting as an oversight mechanism.

3. Article 8 ECHR and Surveillance

The ECtHR has been deciding cases on surveillance since the 1970s. These cases have predominantly focused on targeted surveillance and the Court has developed a thorough and consistent approach to these cases. The Court is only just beginning to deal with bulk surveillance cases, and even then, not with the most contemporary forms of communication. There are many issues and areas of interest left for the Court to address provided by contemporary communications such as social media. The aim of this chapter is to outline Article 8 ECHR and in doing so outline the Court's approach to targeted surveillance. Following this the chapter discusses the Court's approach to justifying interferences with Article 8, showing how the covert nature of surveillance combined with developments in technology has placed the Court's approach in a difficult bind. This is part of a larger trend where the Court's historic approach to surveillance is not equipped for the demands of today both in terms of procedure and substantive principles.

3.1 Article 8 ECHR

Before proceeding to examine the Court's approach to examining interferences with Article 8 it is necessary to first set out a brief summary of said article. Article 8 ECHR enshrines the right to respect for a person's private and family life. The text of Article 8 reads as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 guarantees to everyone a sphere of privacy and personal autonomy generating both positive and negative obligations for Contracting States. The scope of this right has expanded substantially over the years to cover a broad range of interests. These include: informational privacy, personal identity, physical and psychological integrity and relationships with others

and the outside world.[1] Correspondingly, there is an enormous body of jurisprudence involving the Article 8(1) right.

At the same time, Article 8 is a qualified, not an absolute, right. According to Article 8(2), limitations on the Article 8 right are permitted in pursuit of one of the stated objectives. However, any interference with Article 8 in purported pursuit of one of these legitimate aims must meet the requirements of lawfulness and necessity. In order to meet the requirement of lawfulness the interference with the Convention Right must be 'in accordance with the law'.[2] This expression not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law.[3] In particular the law must be clear, foreseeable and adequately accessible.[4] Specifically the law must be sufficiently foreseeable to enable individuals to act in accordance with the law.[5] In terms of necessity, the interference must be necessary in a democratic society to achieve the legitimate aim pursued.[6] This requirement is often framed as the requirement of 'proportionality' or the requirement of a 'fair balance'.[7]

Following this summary of the Article it is useful to begin by discussing how the Court establishes admissibility in practice. This is particularly worth discussing in the context of surveillance due to the difficulty the covert nature of surveillance poses to proving victim status.

3.2 Admissibility: Victim Status and Effective Domestic Remedies

Generally, interferences with Article 8 stem from the negative obligation on states not to interfere with the right. Obvious examples include when a local authority takes a child into care,[8] when a person is dismissed from military services due to being homosexual,[9] or when an immigrant is deported.[10] It is for the applicant to prove that there has been an interference with Article 8. The standard of proof is high in that facts must be proven 'beyond reasonable

[1] Karin De Vries, 'Right to Respect for Private and Family Life' in Van Dijk et al (eds.) *Theory and Practice of the European Convention On Human Rights* (Intersentia 2018) p 667.
[2] Klaus Müller v. Germany, no. 24173/18, 19 November 2020 paras 48 – 51.
[3] Halford v. the United Kingdom, 25 June 1997, Reports of Judgments and Decisions 1997-III para 49.
[4] *Silver and Others v. the United Kingdom*, 25 March 1983, Series A no. 61 para 87.
[5] *Lebois v. Bulgaria*, no. 67482/14, 19 October 2017 paras 66 – 67.
[6] *Z v. Finland*, 25 February 1997, Reports of Judgments and Decisions 1997-I para 94.
[7] *Gaskin v. the United Kingdom*, 7 July 1989, Series A no. 160 para 42, *Roche v. the United Kingdom* [GC], no. 32555/96, ECHR 2005-X para 157.
[8] *K and T v Finland* 2001-VII; 36 EHRR 255 GC.
[9] *Smith and Grady v UK* 1999-VI; 29 EHRR 493.
[10] *Boultif v Switzerland* 2001-IX; 33 EHRR 1179.

doubt'.[11] *Kurt v Turkey* concerned the alleged destruction of the applicant's home by Turkish security forces.[12] However, the applicant didn't submit an eye-witness statement, couldn't provide any particulars as to the identity of the soldiers and it couldn't be determined whether the houses shown in pictures provided by the applicant had been burnt down or merely collapsed for other reasons. The Court thus held that the required standard of proof had not been met and there was therefore no violation of Article 8.[13]

While Article 8 cases generally concern negative obligations, the Court has acknowledged positive obligations on occasion. While the Court referred to positive obligations in the *Belgian Linquistics,* the particular view that the need for States to effectively safeguard Convention rights could require governmental authorities to undertake positive actions stems from *Marckx v Belgium*.[14] Often positive obligations arise regarding recognition of the sexual identity of the person,[15] the right to know one's origins,[16] and the right to one's image.[17] In terms of the social aspect of private life the Court has been less forthcoming in terms of positive obligations.[18] Likewise, in terms of respect for correspondence there are very few cases where the Court imposes a positive obligation on the Contracting Parties. One example is *Cotlet v. Romania*, in which the Court found that Article 8 places a positive obligation on the prison authorities to provide detainees with the ability to correspond with the Court.[19] It is fair to state that thus far the Court has found little reason to impose a positive obligation in how it interprets Article 8 in the context of surveillance.

Positive obligations appear to be a fruitful avenue for the Court to pursue in context of surveillance. There are two forms of positive obligations, first there is an obligation to put in place a legislative framework to ensure the full realisation of Article 8 rights. Second there is an obligation to prevent violations of Article 8 rights by third parties. Such as in *Von Hannover v Germany* where the Court held that it was incumbent on states to ensure that the right of person under their jurisdiction to their image is respected by third parties. In the context of surveillance this could provide an avenue for the Court to address the privacy

[11] *Sekanina v. Austria,* 25 August 1993, § 25, Series A no. 266-A.
[12] *Nuri Kurt v Turkey* (2007) 44 EHHR 36.
[13] ibid
[14] A 31 (1979); (1979–80) 2 EHRR 305, Mowbray, Alastair. "The Creativity of the European Court of Human Rights." (2005) 5 Human Rights Law Review 57-79.
[15] See *Christine Godwin v. the United Kingdom, Rees v. the United Kingdom,* and *B v France*
[16] See *Gaskin v. the United Kingdom, Mikuli v Croatia,* and *Odievre v France*
[17] *Von Hannover v. Germany* para 66
[18] See *Botta v Italy* and *Sisojeva and Others v Latvia*
[19] *Cotlet v Romania* (38565/97) (Unreported, June 3, 2003) (ECHR)

issues stemming from social media use and sale of identifiable data as well as sharing that data with governments, such as through the bulk acquisition framework under the IPA 2016.

It is worth noting that the establishment of victim status is different in the context of surveillance due to the covert nature of surveillance and how it is often used in pursuit of the legitimate aim of national security. Surveillance regimes do not normally contain any requirement that the subject of the surveillance be notified that they have been subject to surveillance. This makes the establishment of victim status difficult for the applicant as it is near impossible for them to gather evidence that they have been subject to surveillance.

The Court provided a workaround to this difficulty in *Klass and Others v. Germany*.[20] The case concerned secret surveillance by state authorities involving the opening and inspection of mail and post, reading telegraphic messages, and monitoring and recording telephone conversations. The Court considered that the question of whether such surveillance measures, had been ordered or implemented in respect of the applicants "had no bearing on the appreciation of the applicants' status as victims".[21] In the Court's view the menace of surveillance lay in its ability to restrict free communication through the postal and telecommunication services. Thus it was held that a person could complain of an interference by virtue of the very existence of legislation allowing interception without demonstrating any concrete instances of surveillance.[22] This was qualified in *Zakharov v Russia*,[23] which applied *Kennedy v UK*[24] in stating that this applies only where there are no effective domestic remedies, since in such circumstances widespread suspicion that powers are being abused is justified. Where remedies exist, applicants must satisfy the higher threshold of demonstrating that, as a result of their personal circumstances, they are potentially at risk of having their communications intercepted.[25] As will be seen in the chapter 6 on bulk surveillance case law, this has meant that the court has tended to examine the legislative frameworks surrounding surveillance cases *in abstracto*.

[20] *Klass and Others v. Germany* (1979-80) 2 EHRR 214.
[21] Elisabet Fura and Mark Klamberg, The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA (October 23, 2012). Josep Casadevall, Egbert Myjer, Michael O'Boyle (editors), "Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights", Wolf Legal Publishers, Oisterwijk, 2012, pp. 463-481. Available at SSRN: https://ssrn.com/abstract=2169894.
[22] *Klass and Others v. Germany* (1979-80) 2 EHRR 214 para 34.
[23] *Zakharov v Russia* (2016) 63 EHRR 17 para 171.
[24] *Kennedy v. UK* (2011) 52 EHRR 4 para 109.
[25] *Zakharov v Russia* (2016) 63 EHRR 17 para 171.

The Court considered how the inherent secrecy of surveillance interacts with exhaustion of domestic remedies in *Kennedy v UK*. If a government claims non-exhaustion, it "must satisfy the Court that the remedy proposed was an effective one available in theory and practice at the relevant time, that is to say, that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success".[26] The logic behind this statement pertains to the quality of the available domestic remedy to the personal situation of the applicant. Effectiveness played a large role in the Court's reasoning here as while the IPT was accessible to the applicant it had no real ability to provide redress due to its inability to place a binding obligation on the executive. In *Big Brother Watch v. UK* the applicants attempted to rely on this ruling, arguing that they had not failed to exhaust domestic remedies due to the IPT not being an effective remedy.[27] However, the Court revisited *Kennedy* and determined that the IPT's jurisprudence had developed vastly since then such that its earlier concerns were no longer valid. It thus declared that a failure to bring IPT proceedings renders applications inadmissible unless there are special circumstances.[28] In this instance, there were special circumstances, namely that *Kennedy* was valid when the applicants made their applications. Thus, the Court allowed the applicants to proceed under the special circumstances exception to the non-exhaustion rule.[29]

The judgment in *Kennedy* raises the question of what the Court considers to be an 'effective remedy' in this context. As stated above, the Court did not consider the IPT effective at the time of *Kennedy* but did by the time of *Big Brother Watch*. The Court based this on the development of the Tribunal's jurisprudence. But how exactly had its jurisprudence developed? It is interesting that the Court's appraisal was not based on the powers the IPT had as its powers did not change in the time between the two cases. In *Big Brother Watch* the Court stated that "to be effective, a remedy must be capable of remedying directly the impugned state of affairs and must offer reasonable prospects of success." Specifically, in *Kennedy* the Court had found that the IPT could consider complaints about the general compliance of the surveillance regime with the Convention and could make a finding of incompatibility if necessary. However, such a finding of incompatibility did not give rise to a binding obligation on the Government to remedy said incompatibility to benefit the applicant.

[26] Ibid, para 109.
[27] *Big Brother Watch and Others v. The United Kingdom,* App nos. 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018), paras 262 – 266.
[28] Ibid para 265.
[29] Ibid, para 266.

So, then, in order for the IPT to be considered an effective remedy it would have to have the power to impose a binding obligation on the Government. However, in *Big Brother Watch* the Court held that the practice of the Government giving effect to the IPT's findings on the incompatibility of domestic law with the Convention was sufficiently certain for it to be considered an effective remedy.[30] This seems problematic. The IPT had not been given any increased statutory powers in the years between the two cases. The Court is trusting that the good working relationship between the Government and the IPT will continue. If the next government of the UK takes a harsher stance towards findings of the IPT and refuses to remedy incompatibilities in a timely manner, does it follow that the IPT will return to its *Kennedy* state of ineffectiveness? Such a reliance on the sensible use of discretion is insufficient, as it is subject to change. The Court should have required a specific legally binding guarantee. The Court added in *Big Brother Watch* that the IPT's effectiveness was bolstered by its ability to reference a case, as a matter of EU law, to the CJEU, which could then impose a binding obligation on the UK Government.[31] However, this will not be the case in the future in a post-Brexit UK further strengthening the case for requiring that the IPT be able to impose a legally binding obligation. Leaving aside difficult Brexit related questions, it is clear that establishing victim status in a covert area such as surveillance is difficult.

3.3 Private Life

While Article 8 covers a person's private life, family, home and correspondence this section will discuss the sections most relevant to surveillance: private life and correspondence. Private life is a very broad concept. In the *Belgian Linguistics* case the Court first considered the scope of Article 8, explaining that a case concerning the right of parents of French-speaking children in Belgium to have their children educated in French was essentially about protecting the individual against arbitrary interference by the public authorities in their private and family life.[32] From the beginning the Court eschewed a narrow approach, limited to notions of privacy and protection from publicity, in favour of a broad approach which emphasised the ability to live one's life without arbitrary disruption or interference.[33] This broad approach is underpinned by the concept of effectiveness, and indicates the process of

[30] Ibid para 262.
[31] Ibid para 263.
[32] *Belgian Linguistics* case (No. 2) (1968) 1 EHRR 252.
[33] David John Harris, Michael O'Boyle, Ed Bates, and Carla Buckley. *Harris, O'Boyle & Warbrick: Law of the European convention on human rights*. Oxford University Press, USA, 2014. P504.

evolutive interpretation the Court took with Article 8 from the *Belgian Linguistics* case in the 1960s to today.

In *Niemietz v Germany* the court refrained from providing a comprehensive definition of 'private life':

> The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings … There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.[34]

While the Court refrained from a comprehensive definition, the scope of the concept has expanded significantly over the years as the Court conducted an evolutive interpretation of the right. In *X and Y v Netherlands* it stated that private life is a concept which "covers the physical and moral integrity of the person, including his or her sexual life."[35] This was reaffirmed in *Dudgeon v UK, Norris v Ireland* and *Modinos v Cyprus* regarding the criminalisation of homosexuality.[36] Secret surveillance also comes under the private life aspect of Article 8, specifically concerning the privacy of communications. The case law on secret surveillance will be returned to in more detail in a later chapter[37], however, for the purposes of the current chapter it is useful to set out here what is regarded as secret surveillance. For example, the act of monitoring public spaces through CCTV is not considered secret surveillance. This was addressed by the EComHR in *Pierre Herbecq*. The applicants invoked the potential chilling effect of such surveillance, stating that such surveillance might compel individuals to censor their own behaviour in order to avoid

[34] *Niemietz v Germany* App no. 13710/88 (ECtHR 16 December 1992) para 29.
[35] *X and Y v. The Netherlands* App no. 8978/90 (ECtHR 26 March 1985), para 22.
[36] *Dudgeon v The United Kingdom* App no. 7525/76 (ECtHR 22 October 1981), *Norris v. Ireland* App no. 10581/83 (ECtHR 26 October 1988), *Modinos v. Cyprus* App no. 15070/89 (ECtHR 22 April 1993)
[37] See chapter 6 on "Bulk Interception Case Law of the ECHR".

behaving in a manner which could be interpreted as deviant or illegal by observers using surveillance equipment.[38] However, the Commission found that the behaviour observed was public behaviour and, as such, the information gathered by the cameras would be identical to that that could be obtained by a person present in the same spot.[39]

This is further explained in *P.G & J.H v UK*, where it was stated that a person's reasonable expectations of privacy may be a significant – although not necessarily conclusive – factor in whether there has been a violation of Article 8(1).[40] There are occasions where people knowingly or intentionally involve themselves in activities which may be recorded or reported in a public manner. For example, a person who walks down the street will, inevitably, be visible to any member of the public or may be monitored by a security guard through a CCTV camera. However, the Court stressed that the important issue is whether and how the applicant's information was processed. Private life considerations may arise once any systemic or permanent record comes into existence, even if the methods used to gather said record are not intrusive or covert.[41]

This was supported by the judgment in *Peck v UK*, which concerned the monitoring of CCTV footage to stop a man from attempting to commit suicide. The applicant did not submit that the monitoring of his activity on CCTV was an interference and the Court – referencing the judgment in *P.G & J.H.* – confirmed that it was not. However, the storage and disclosure of these images in a press release was.[42] Specifically, the violation lay in the lack of sufficient safeguards to prevent disclosure of said images to media outlets. The disclosure therefore constituted a disproportionate and unjustified interference with Peck's private life and a violation of Article 8.[43] This was echoed in *Catt v UK*, in which the Court stated that the mere storage of information can amount to an interference with the applicants' right to respect for private life.[44] Although it should be noted that *Catt* concerned the storing of information about the applicant's political life, which led to increased strictness on the part of the Court.[45] It is unlikely that the storage of any type of information will give rise to a violation of Article

[38] *Pierre Herbecq and the Association Ligue des droits de l'Homme v Belgium* App no. 32200/96 and 32201/96 (ECtHR 14 January 1998) p 97.
[39] Ibid.
[40] *P.G & J.H v UK* (2008) 46 EHRR para 57.
[41] ibid, para 60.
[42] *Peck v UK* (2003) 36 EHRR 41 para 59.
[43] Ibid, para 87.
[44] *Catt v UK* (2019) 69 EHRR 7 para 93.
[45] Elvin Abbasli "The Protection of the Freedom of Expression in Europe: Analysis of Article 10 of the ECHR." (2015) 2 Baku St. UL Rev 18.

8. *Catt* cannot be read as a blanket principle that storage of info gives rise to an interference with Article 8.

The Court's approach is based largely then on whether there is a reasonable expectation of privacy, with consideration also given to any creation of systemic or permanent records. However, it is not clear how this approach interacts with contemporary social media. The reasonable expectation of privacy varies from platform to platform as what may be viewed publicly on one platform is locked behind invite only groups or only available to friends on others. Social media posts and data are effectively systemic or permanent records created by users and stored by various platforms. How does the Court's approach interact with contemporary social media platforms? Does a social media profile being locked affect the individual's reasonable expectation of privacy in the Court's eyes? Or does the use of social media at all bring with it a lowered expectation of privacy? With regard to the creation of systemic or permanent records, does the user's creation of their own record, their profile, negate this consideration? If the social media company shares this profile with a government agency, does this give rise to an interference? This highlights a number of future issues for the Court to address which will be returned to in later chapters but for now it is useful to think of an example. Suppose that someone runs an open personal Twitter account, claiming to be a member of a politically controversial, but not proscribed, group. Does the fact that anyone can follow and view the account mean that it is considered public in terms of privacy expectations? Does a government agency using the Twitter API to download my tweets give rise to a privacy consideration? How does this interact with the right to be forgotten as I now have no means to fully delete all instances of that personal data?[46] Now, what if I have a second Twitter account which is locked, meaning that it cannot be viewed or followed without my permission. Is this a private space? The intelligence agency subjecting me to surveillance may feel that it is more necessary to have access to these tweets as they may be of increased intelligence value. In order to access this data GCHQ would likely request this data directly from Twitter. Does the provision of this data by Twitter give rise to an interference? If *Catt* applies then the interference does not occur when the user consents to giving his data to Twitter but the mere storage of said data by a state entity would give rise to an interference. This depends on the content of the data however, as the Court discerns between political and non-political data. Separately, there is also the act of Twitter sharing

[46]Jeffrey Rosen. "The right to be forgotten." (2011) 64 Stan. L. Rev. Online 88

my data with the SIA, the Court may see a positive obligation for the State to ensure the effective protection of Article 8 rights through the implementation of a legal framework for this action.

Or to use an example closer to the issue of combatting terrorism online. Telegram is a social media platform which utilises encrypted one-to-one and one-to-many communications. It is clear to see that an encrypted one-to-one Telegram communication carries with it a reasonable expectation of being private. The complication comes from the one-to-many communication which has been historically popular with both ISIS[47] and Neo-Nazis[48] organising on the platform. These channels, which enable mass communication, can either be open or closed. The logic of the lack of privacy expectation is clear on an open channel; think of a public forum in Ancient Athens where individuals could go and listen to what the speaker had to say. In such a situation the expectation of privacy would be low. However, the channels employed by terrorist groups on the platform are often closed in order to avoid scrutiny, and one must be permitted to join in order to access the communications. It is difficult to say whether there is a reasonable expectation of privacy here. The channel is private in the sense that it is locked off from the public, but these groups can contain hundreds if not thousands of people. A suitable example might be the Jacobin Clubs in the build up to the French Revolution. In order to attend the meetings one had to be invited in, but again the meetings contained multitudes of people. What was the expectation of privacy within such a meeting? The Jacobins likely feared infiltration and surveillance by spies in the same way ISIS and Neo-Nazi groups on Telegram do. This raises the question whether this expectation of privacy is reasonable. With respect to Telegram channels used by these proscribed groups, the steps taken by said groups to ensure privacy may suggest that their expectation is reasonable. However, the subject matter being discussed in these private groups may be known to be of interest to intelligence and law enforcement, rendering the expectation unreasonable. So then while the data obtained and stored is of a political nature and would likely give rise to an interference under Article 8, it would likely be justified as being within the respondent state's margin of appreciation in pursuit of a legitimate aim in national security as will be discussed later in this chapter.

[47] Nico Prucha, 'IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram'(2016) 10 Perspectives on Terrorism 6.
[48] Michael Colborne, 'Revealed: The Ukrainian Man Who Runs A Neo-Nazi Terrorist Telegram Channel' (*Bellingcat,* 18/03/2020) <https://www.bellingcat.com/news/2020/03/18/revealed-the-ukrainian-man-who-runs-a-neo-nazi-terrorist-telegram-channel/> accessed 07/06/2022.

Departing from the expectation of privacy arguments, when will the storage and aggregation of nominally publicly available data constitute an interference with the right? In *Catt* records of the applicant's attendance at political rallies and protests gave rise to an interference with Article 8.[49] In the 2006 *Segerstedt-Wiberg* case the court applied a proportionality test to the type of information held by the Swedish secret police on each of the five applicants.[50] The information on the first applicant pertained to how they had been the target of a 1990 letter bomb campaign. The Court held that holding this information was proportionate to the aim of keeping the individual safe. Thus, there was no violation of Article 8. For the remaining four applicants, the Court found unanimously that there had been violations of Article 8 owing to the interferences being disproportionate. The second and fifth applicants' information referred to peaceful political activities in the late 1960s. The Court held that the age and nature of the information meant there were not sufficient reasons to justify continued storage.[51] The information on the third and fourth applicants related to their ongoing membership of the "Marxist-Leninist (revolutionaries) Party". The Court explained that, although the programme of the party endorsed the principle of armed opposition, it didn't make an unequivocal call for the use of political violence. The Court also explained that it was necessary to consider the words and actions of the party leaders, information which the respondent State hadn't provided. A party programme alone wasn't a sufficient reason to justify continued storage of the information. The Court also found that the storage of information on political activities violated Article 10 and the lack of a domestic remedy to delete said information violated Article 13.[52]

Catt and *Segerstedt-Wiberg* broadly refer to the right to be forgotten and raise questions for the Court to answer going forward. From these cases we can see that there is a limit on how long the State can keep records on your political activity, and that the Court is willing to be nuanced about membership to controversial political parties based on the group's endorsement of political violence. However, in *Segerstedt-Wiberg* the Court denied the first applicant's claim because the reason their information was recorded was that they were in danger themselves. This is a contentious decision as it denies the right to be forgotten to an individual due to their having being targeted 16 years prior. This raises questions when applied to the social media realm. First, what is the time limit for storing information

[49] *Catt v United Kingdom* (2019) EHRR 7 para 114.
[50] *Segerstedt-Wiberg v Sweden* (2007) 44 EHRR 2 para 89.
[51] Ibid para 90.
[52] Ibid para 91.

collected online? The Court has stressed how information about an event which was initially public becomes a part of a person's private life as it "recedes into the past".[53] In *Segerstedt-Wiberg* the Court held that roughly 30 years was too long, but this seems too long a duration for contemporary technology, especially when a user may decide to delete their own social media posts or profiles they do not politically identify with anymore. While this ruling gives the upper limit on this duration it leaves the question of what the appropriate duration is for contemporary technology. Should there be an additional duty on Governments to delete their records of posts that the original author has since deleted? A less serious example of this would be the practice on Twitter of searching the early posts of newly popular users in order to discredit them for their previous controversial opinions. This often leads to users being attacked for opinions posted over a decade prior. Though this is an often ineffectual activity of individuals with little power on a social media platform, the consequences of such a practice if utilised by governments is much more serious.

Second, membership of which groups necessitates ongoing storage of political data? From *Segerstedt-Wiberg* it seems that the test for a political party is whether it unequivocally endorses political violence, with consideration of the views and actions of the leaders of the party. Believing in the necessity of violence in principle is not enough. This may be a non-issue when it comes to membership of proscribed groups such as those espousing terrorism but is less clear for those on the fringes, such as far right nationalist groups which seek power through electoral means. This link becomes more tenuous when brought online as membership in a group is not easily proven. If we return to the Telegram example, does membership of a channel dedicated to an extremist group equate to membership of said group for the purposes of aggregating data on a user? Terrorism scholars peruse these channels in the course of research, which may lead to their data being collected automatically or inadvertently by surveillance authorities. It is clear that the application of offline scenarios to online is providing the Court with more and more issues to resolve in the future. These scenarios will become further complicated given the mismatch between contemporary surveillance practices and their associated safeguards, which will be returned to in chapter 6.

3.4 Correspondence

[53] *MM v United Kingdom* App no. 24029/07 (ECtHR 13 November 2012) para 188, *Rotaru v Romania* App no. 28341/95 (ECtHR 4 May 2000) paras 44 – 45.

There are also outstanding issues for the Court to address when one examines correspondence. Article 8 guarantees the right to respect for one's correspondence. Correspondence has been interpreted by the Court as including more modern methods of communication, such as e-mail[54] and the monitoring of workplace internet computer usage.[55] Additionally it includes professional correspondence such as messages between lawyers and their clients.[56] Cases concerning interferences with this right often concern the intercepting, monitoring and examination of correspondence by public authorities without the permission of the person or people concerned.[57] These interferences often occur in the course of criminal investigations. Where secret surveillance methods are used, the right to private life is often also at stake.[58]

In a number of cases, this right has concerned the interception of detainees' correspondence with the outside world. This right is of particular significance to these individuals as their letters, emails and telephone calls form important means of maintaining contact with the outside world and providers of legal aid.[59] The Court found a violation of Article 8 in *Golder v UK* where the applicant wished to submit a complaint about his treatment by prison staff but was prevented from contacting his lawyer.[60] Another violation was found in *Schonenberger and Durmaz v Switzerland* where a letter sent from a lawyer to his client was stopped by the public prosecutor.[61] In *Szuluk v UK* it was found that detainees suffering from serious illnesses must be able to contact medical specialists without restrictions from the prison's medical personnel.[62]

However, this does not mean that monitoring of such correspondence is completely forbidden. The Court has accepted that it may be necessary to conduct such monitoring, but it must be necessary in view of the pursued aim. These interferences must also be based on rules that are "sufficiently clear and detailed to afford appropriate protection against arbitrary interference".[63] In the case of *Buglov v. Ukraine* the Court found that the prison authority's

[54] *Copland v United Kingdom* App no. 62617/00 (ECtHR 3 April 2007).
[55] *Barbulescu v Romania* App no. 61496/08 (ECtHR 5 September 2017).
[56] *Michaud v. France* App no. 12323/11 (ECtHR 6 December 2012) paras 117 – 119.
[57] *Szuluk v. the United Kingdom* App no. 36936/05 (ECtHR 2 June 2009), *Campbell v. the United Kingdom* (1992) 15 EHRR 137, *Piechowicz v. Poland* App no. 20071/07 (ECtHR 17 April 2012).
[58] Karin De Vries, 'Right to Respect for Private and Family Life' in Van Dijk et al (eds.) *Theory and Practice of the European Convention On Human Rights* (Intersentia 2018) P 732.
[59] Ibid
[60] *Golder v. the United Kingdom* (1979-80) 1 EHRR 524 paras. 43-45.
[61] *Schonenberger and Durmaz v. Switzerland* (1989) 11 EHRR 202 paras. 24-30.
[62] *Szuluk v. the United Kingdom* (2010) 50 EHRR 10 para. 53.
[63] *Doerga v. the Netherlands* (2005) 41 EHRR 4, para 53.

monitoring of the individual's correspondence was not necessary for the aim of preventing the obstruction of the course of justice.[64] Later in the same judgment the Court found that placing the applicant in a disciplinary cell for bypassing the prison administration when sending a complaint about his conditions was not proportionate.[65]

The Court has kept up with technological change in its jurisprudence on surveillance to a certain point. Unsurprisingly, the Court is yet to address more contemporary forms of communication, such the interception of communications on social media platforms or messaging apps such as Whatsapp or Telegram. This can be attributed to the time it takes for cases to be brought before the Court. There may be a case on social media surveillance within the next decade but the danger is that by then this too will be obsolete. Such a future case might focus on the specific characteristics of today's most-used platforms, such as Facebook, Twitter or YouTube but by such a time users may be moving onto new platforms as they did before in their moves from MySpace and Bebo to the aforementioned platforms.[66] Regardless of which platforms are most popular, the functionality of platforms will have progressed, providing further issues for the Court to address. The Court's view of what is covered by Article 8 is, therefore, one which is confounded by both the covert nature of surveillance, in terms of establishing victim status, and by the speed of technological change both in terms of surveillance technology and the technologic milieu surrounding it. There two problems are also evident in the Court's approach to interferences with Article 8.

3.5 Justifications for Interference with Article 8

Article 8 is a qualified right and interferences are permitted in pursuit of certain legitimate aims such as national security or public safety. These interferences must meet the requirements of lawfulness and necessity. Lawfulness in this context means that said interference must have a basis in domestic law, and said basis must be accessible and foreseeable to the public. The interference must be necessary in a democratic society to achieve the pursued legitimate aim. The Court has stated on several occasions that the object of Article 8 is "essentially that of protecting the individual against arbitrary interference by the public authorities in his private or family life"[67]. It follows that for an interference with

[64] *Buglov v. Ukraine* App no. 28825/02 (ECtHR 10 July 2014) para. 130.
[65] Ibid., para. 132.
[66] Mojtaba Torkjazi, Reza Rejaie, and Walter Willinger. "Hot today, gone tomorrow: on the migration of MySpace users." (2009) In *Proceedings of the 2nd ACM workshop on Online social networks*, pp. 43-48.
[67] *X and Y v. The Netherlands* (1986) 8 EHRR 235 para.23

the right to be justifiable, it must not be arbitrary and therefore consistent with respect for the individual's private sphere. In addition, interference is only permissible within the limits specified in Article 8(2): if it exceeds these limits it is a violation of the individual's right to respect for his private sphere. Article 8 thus imposes on Contracting States a negative obligation: in order to secure the right guaranteed by Article 8, states must abstain from unjustified interference in the private sphere.[68] While Article 8 does generate positive obligations, thus far this has not occurred in the surveillance context. Thus, the focus of this section will be the Court's approach in relation to negative obligations. This section begins by exploring the Court's general approach to Article 8 before focusing fully on the Court's approach to surveillance.

3.5.1 In Accordance with the Law

The Court has established a threefold test for determining whether an interference was in accordance with the law. First, it must be established that interference with the Convention right has some basis in domestic law. Second, the law must be accessible, and third the law must be foreseeable. The latter requires that the law is formulated in such a way that a person can foresee, to a degree that is reasonable in the circumstances, the consequences which a given action will entail.[69] Accessibility and foreseeability have been referred to as the 'quality of law' requirements.[70] In the *Sunday Times*[71] Article 10 case the Court stated that it was not enough that the interference into the Convention right had a basis in law, the character of the law also played a significant role.

The terms 'in accordance with law' refers to national law. In general, the Court must accept the interpretation of national law adopted by the national courts, barring very strong reasons for disagreeing. This is not because the Court isn't a fourth instance court but because questions of national law are treated as matters of fact by the Court.[72] Sometimes the Court has taken a more interventionist approach, as in *Zaiet v Romania.*[73] Since in the ECHR system law is comprised of written and unwritten law,[74] the basis in domestic law also

[68] Connelly, A. M. "Problems of interpretation of Article 8 of the European Convention on Human Rights." International & Comparative Law Quarterly 35, no. 3 (1986): 567-593.
[69] *Fernandez Martinez v Spain* [GC] (2015) 60 EHRR 3 s 117.
[70] *Kennedy v UK* para 151, *Zhakarov v Russia* para 229.
[71] *Sunday Times v United Kingdom* (1979-80) 2 EHRR 245
[72] Bernadette Rainey, Elizabeth Wicks, and Clare Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights* (7th edn, OUP 2017) 343.
[73] *Zaiet v Romania* (2016) 62 EHRR 9.
[74] *C.R. v UK* (1995) Series A no 335-C, par 33.

doesn't need to be statutory, such as in *Sunday Times*,[75] *Slivenko*,[76] and the *Bosphorus Airways* case.[77]

In terms of accessibility, the Court has acknowledged that States do not have to make public all the details of the operation of a secret surveillance regime, provided that sufficient information is available in the public domain.[78] In the context of secret surveillance, it is inevitable that "below the waterline" arrangements will exist, and the real question for the Court is whether it can be satisfied, based on the "above the waterline" material, that the law is sufficiently foreseeable to minimise the risk of abuses of power. Here then the foreseeability requirement is used in place of the accessibility requirement. The Court has noted that the existence of 'below the waterline' material has the potential to undermine any attempt to assess the foreseeability and necessity of a secret surveillance regime.[79] After all, it is questionable whether it is possible to assess the sufficiency of the 'above the waterline' material, when the nature and extent of the 'below the waterline' material is unknown.

In terms of foreseeability individuals must be able to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. The Court added in the Article 10 *Sunday Times* case that the requirement of foreseeability was not designed to secure absolute certainty, so that no interpretation would be required in determining the scope of application of the law. However, in *Vogt* the Court held that the level of precision required "depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed."[80]

A good example of an Article 8 case failing the foreseeability requirement is *Silver v UK*, concerning prisoners complaining that the stopping and delaying of their mail by the prison authorities amounted to a breach of Article 8.[81] The UK had detailed rules governing correspondence to and from prisoners, but these were stored in confidential internal administrative guidance, issued by the Home Secretary to prison governors. Some of the rules were disclosed to prisoners via cell cards. Thus, there was no dispute that the impugned

[75] *Sunday Times v United Kingdom* (1979-80) 2 EHRR 245.
[76] *Slivenko v Latvia* (2004) 39 EHRR 24.
[77] *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi v Ireland* (2006) 42 EHRR 1.
[78] *Zakharov v Russia* (2016) 63 EHRR 17 para 243 – 244.
[79] *Big Brother Watch and Others v. The United Kingdom,* App nos. 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018), para 325.
[80] *Vogt v Germany* (1996) 21 EHRR 205 para 2(b).
[81] *Silver and Others v United Kingdom* (1981) 3 EHRR 475.

measures had a basis in domestic law. The Prison Act 1952 and its accompanying rules were held to be accessible. The legislation in question allowed for some discretion however "the Court has already recognised the impossibility of attaining absolute certainty in the framing of laws and the risk that the search for certainty may entail excessive rigidity".[82] But, upon examining the circumstances surrounding the censorship or delaying of the applicant's mail, the Court held unanimously that there had been a violation of Article 8. There was a detailed set of rules which governed how the prisoners' mail could be checked but these were kept secret. Accordingly, the circumstances in which their mail would be subject to censorship or delay were held to be unforeseeable to the prisoners.

In the context of surveillance, both the applicants and the Court often resort to in accordance with law arguments as opposed to necessity or proportionality arguments. There are several plausible reasons for this. One is that the Court focuses on them for the simple reason that they are easier requirements to check.[83] Testing in accordance with law requirements avoids direct competition between individual rights and the public interest in such a complex and sensitive area.[84] In such an area the balance struck between competing goals and interests "will inevitably reflect a value choice, but not one which purports to eradicate the initial conflict."[85] Considering the context of national security which surveillance cases operate, it is not surprising that the Court avoids striking such a balance. In *Malone* the Court stressed that the law must indicate the scope of any discretion of the executive with regard to the interception of communications and the manner of its exercise with sufficient clarity to give the individual protection against arbitrary interference. The Court held that the common law of England and Wales on the subject was so obscure and subject to such differing interpretations that it did not qualify as law in the eyes of the Convention.[86] In the joined cases of *Kruslin v France*[87] and *Huvig v France*,[88] the court stated that tapping and other forms of interception represent a serious interference with private life and correspondence and accordingly must be based on a law that is particularly precise. It is essential to have

[82] Ibid para 88.
[83] *Blanca R Ruiz, "Privacy in Telecommunications. A European and an American Approach" (The Hague: Kluwer Law International, 1997), p.181.*
[84] Maria Helen Murphy, A Shift in the Approach of the European Court of Human Rights in Surveillance Cases: A Rejuvenation of Necessity?'(2014). 5 EHRLR 515.
[85] Aileen McHarg, "Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights" (1999) 62(5) M.L.R. 671 at 677.
[86] *Malone v United Kingdom* (1985) 7 EHRR 14.
[87] *Kruslin v. France* (1990) 12 EHRR 547.
[88] *Huvig v. France* (1990) 12 EHRR 528.

clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated. In *Halford v UK* the complete lack of a regulatory framework for the surveillance of employees' telephones in a private exchange by the police was found to be not in accordance with the law.[89]

The Court's approach to the in accordance with the law test is best explained by examining the case of *Kruslin v France* in closer detail. The Court first conducted the 'basis in domestic law' step of the 'in accordance with the law' test, finding that the interference had a legal basis in French law.[90] Following this the Court proceeded to the 'quality of the law' requirements, finding that the accessibility of the law did not raise any problems in the instant case. Foreseeability was where the bulk of the Court's deliberation fell.[91]

The Government attempted to invoke the subsidiary nature of the Court by submitting that the Court must be careful not to rule on whether French legislation conformed to the Convention in the abstract, and that they should not decide upon legislative policy. The Court, the Government submitted, should be concerned with the facts of the case before it, specifically the tapping of the applicant's communications. It followed that the key issue in this regard was whether the interference with the Article 8 right was necessary. The Court rejected this argument, stating that it must ascertain whether the interference in question was "in accordance with the law" and it must therefore assess the relevant law in force at the time of the interference.[92] This highlights the tension between subsidiarity and effectiveness the Court is attempting to resolve in surveillance cases through the use of the in accordance with law test. While the French government intended to direct the case towards the necessity test where they could rely on their margin of appreciation, the Court held that it must first examine the quality of law. The Court then found a violation of the French law without requiring an assessment of the necessity.

The Court first stated that tapping and other forms of intercepting telephone communications represent a serious interference with private life and correspondence and must accordingly be based on a law that is particularly precise: "It is all the more essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming

[89] *Halford v UK* (1997) 24 EHRR 523 para 32.
[90] *Kruslin v. France* para 28.
[91] Ibid para 30.
[92] Ibid para 31.

more sophisticated."[93] Next the Court pointed to the safeguards present in the French law; authorisation and supervision by an independent judicial authority, the lack of subterfuge or ruses involved in the interception and the protection of communications between the accused and lawyer. However, the Court noted that few of these safeguards were expressly provided for in the Code of Criminal Procedure, with the remainder derived piecemeal from judgments, or not expressly laid down in case law at all. Rather the Government inferred them from interpretations of general principles, legislative provisions, and court decisions. This did not provide the required legal certainty.[94]

Most importantly the French system did not afford 'adequate safeguards against various possible abuses.'[95] Categories of people liable to have their telephones tapped and the nature of offences which may give rise to an interception order were not defined. There was no obligation for the judge in question to set a limit on the duration of tapping. The Court thus found that the French law did not indicate with reasonable clarity the scope and manner of discretion conferred on the public authorities. Additionally, at the time of the interference the applicant didn't enjoy the minimum degree of protection which citizens are entitled to under the rule of law. Following this, the Court did not consider it necessary to review the purpose and necessity of the interference. This was done for two reasons: first the Court almost always takes the approach of not discussing issues that have been rendered redundant by its conclusions on prior issues. Second, having found that the law is too vague or uncertain to determine what it actually is, it would be impossible for the Court to then assess its necessity.

However, this contributes to the lack of analysis by the Court in general of the purpose and necessity of the police intercepting a suspect's communications.[96] In *Kruslin* the presence of adequate safeguards against abuse was treated as being a part of the 'in accordance with the law' test but in other cases such as *Klass* and *Leander* it was viewed as a fundamental aspect of the necessity test, as will be seen later in this chapter. This points to the importance of the adequate safeguards against abuse test within the Court's approach which will be a constant from targeted surveillance case law through to contemporary bulk surveillance case law. This will be returned to in chapter 6 on Bulk Surveillance.[97]

[93] Ibid para 33.
[94] Ibid para 36.
[95] Ibid para 35.
[96] The Court also didn't conduct a necessity test in *Mustafa Sezgin Tanrukulu v. Turkey* 27473/06, [2017] ECHR 669.
[97] See chapter 6 on "Bulk Interception Case Law of the ECHR".

Through this case and the cases proceeding it the growing importance of the 'in accordance with the law' requirements, and more specifically the adequate and effective safeguards against abuse test, can be seen. The Court is faced with a near impossible situation in attempting to provide effective and practical protection of the right of privacy in the face of surveillance measures. These surveillance measures are often justified by real threats to national security, and the Court is cognisant of its subsidiary position to its signatory nation states. Deciding upon the necessity of these bulk surveillance measures requires a political choice which the Court simply does not have the capacity to do. In lieu of this the Court has focused on foreseeability requirements such as the adequate and effective safeguards against abuse test which enable it to hold surveillance regimes to account and minimise the intrusion on an individual's Article 8 rights.

3.5.2 Pursuit of a Legitimate Aim

The second requirement under Article 8(2) provides that the interference must pursue one of certain listed interests in order to be legitimate: national security, public safety or the economic well-being of the country, prevention of disorder or crime, protection of health or morals or the protection of the rights and freedoms of others. Once the Court has established that the law in question is in accordance with the law, it will then consider whether the restriction is for one of the specified legitimate aims.

The Court has tended to avoid deciding cases on this ground.[98] An example is *Weber and Saravia v Germany*, where the Court shared the German Government's view that the aim of the impugned provisions of the amended act in question "was indeed to safeguard national security and/or to prevent crime" and did not "deem it necessary to decide whether the further purposes cited by the Government were also relevant."[99] Additionally in *Leander v Sweden* the stated aim – to protect national security – was described as "clearly a legitimate one for the purposes of Article 8" and thus the main issues of contention were whether the interference was "in accordance with the law" and "necessary in a democratic society".[100] In *Khorosenko v Russia* the Court had reservations as to whether the isolation of prisoners from family visits was in pursuit of a legitimate aim but did not regard it as necessary to decide this point when finding that the interference with Article 8 was not necessary in a democratic

[98] Janneke Gerards. "How to improve the necessity test of the European Court of Human Rights." International journal of constitutional law 11, no. 2 (2013): 466-490., p 480.
[99] *Weber and Saravia v. Germany* App no. 54934/00 (ECHR, 29 June 2006), para 104.
[100] *Leander v. Sweden* (1987) 9 EHRR 433.

society. It is important to note that the Court does not neglect this requirement, the test is very broad and unless the respondent state is acting in clear bad faith it is difficult to find a violation in it. For similar reasons, applicants do not often challenge the respondent state on these grounds. In general the Court attempts to account for this by its adoption of a rigorous approach to the issue of necessity and proportionality in relation to the measures take to secure the legitimate aim.[101]

There is a question of what it would look like for the Court to interrogate more closely whether a given action was in pursuit of a legitimate aim. Is it a question of intent or result? For example, if it turned out that surveillance was not effective for protecting national security through being ineffective at detecting terrorists, would that mean that surveillance was not in pursuit of a legitimate aim? Or is the fact that the government intended for surveillance to assist in the protection of national security sufficient? However, this may be treading onto the territory of the necessity test. This complexity which emerges when one examines the legitimate aim test may explain the Court's aversion to focusing on it in the case-law. In practice the Court solves this complex problem by accepting very general and abstract aims, such as national security. This easy acceptance of broad legitimate aims means that the legitimate aim test doesn't add anything substantial to the Court's approach in deciding between conflicting rights and interests.[102] This then spills over into the necessity requirement as if the aim of the measure is not spelt out very carefully, then this hinders efforts to assess its necessity. This is similar to the effects of "below the waterline" provisions as it is very difficult to assess the necessity of a power if the power is to some extent unknown. This is further complicated by the fact that the extent of what is unknown is itself unknown. Additionally, it is difficult to conduct a proportionality test on the basis of wide aims such as protecting national security which may explain why the Court has decided to sidestep and limit the importance of the 'necessary in a democratic society' test, as the next section explains. However, like the Court's reliance on foreseeability and balancing, this may also be explained by the subsidiary position of the Court. The Court and Contracting Parties may feel, rightly or wrongly, that it is not the Court's role to decide what is essentially a political issue.

[101] Bernadette Rainey, Elizabeth Wicks, and Clare Ovey, *Jacobs, White and Ovey: The European Convention on Human Rights* (7th edn, OUP 2017) 343.
[102] Janneke Gerards. "How to improve the necessity test of the European Court of Human Rights." International journal of constitutional law 11, no. 2 (2013): 466-490., p 480.

3.5.3 Necessary in a Democratic Society - Components

In addition to being in accordance with law and being in pursuit of a legitimate purpose, the restriction in question must also be necessary in a democratic society. The classic formulation of the necessity found in *Sunday Times* was discussed in the previous chapter. The necessity test of the ECHR has been accused of using non-transparent terminology and tending to confuse and mix distinct elements of judicial review.[103] For an interference to be considered necessary in a democratic society in pursuit of a legitimate aim it must address a "pressing social need" and, in particular, it must be proportionate to the legitimate aim pursued and the justifications adduced by the national authorities must be "relevant and sufficient".[104]

This is quite a dense formula. The 'pressing social need' means that the infringement of the right cannot simply be in pursuit of a legitimate aim, the aim must also be pressing.[105] In the *Campbell* case Campbell, a convicted murderer, complained that his correspondence with his lawyer was opened and read by prison authorities. The Court concluded that while this interference was in accordance with the law and had the legitimate aim of preventing crime, it was not necessary in a democratic society as there was no pressing social need to open and read Campbell's correspondence with his solicitor. The opening of said mail could be justified in order to determine whether it contained anything illicit, but this did not justify reading the letter. Opening the mail in the presence of the prisoner would allow for this as it was a less intrusive way of achieving the objective. Reading such privileged correspondence could only be justified when the authorities had reasonable cause to believe that said privilege was being abused. Additionally, there is an assessment of effectiveness since a measure has to correspond to its aims, and if the measure doesn't contribute enough to the achievement of a certain goal the reasons for introducing it are unlikely to relevant and sufficient.

Finally, it is difficult to explain how the presence of a proportionality requirement relates to a pressing social need.[106] It is easier to break up proportionality into two forms. First there is proportionality as a metaphorical scales wherein a 'fair balance' must be struck between the right of an individual applicant and the general interests of the public.[107] In *Soering v UK* the

[103] Ibid p 467.
[104] *Silver and Others v UK* (1983) 5 EHRR 347
[105] Janneke Gerards. "How to improve the necessity test of the European Court of Human Rights." International journal of constitutional law 11, no. 2 (2013): 466-490., p 467.
[106] Ibid.
[107] Yutaka Arai-Takahashi, "The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR" (Antwerp: Intersentia, 2002), p 193.

Court stated that "inherent in the whole of the Convention is a search for a fair balance between the demands of the general interest of the community and the requirement of the protection of the individual's fundamental rights".[108] This is echoed in *Sporrong and Lonnroth v Sweden* concerning the balance of interests inherent to the expropriation of property for redevelopment.[109] Secondly, there is a modified and more specific version of proportionality which is defined as a reasonable relationship between the means employed, including their severity and duration, and the public objective to be sought.[110] It would be obviously disproportionate to use a sledgehammer to crack a walnut. Chapter 6 on bulk surveillance cases will examine which form of proportionality the Court is referring to in bulk surveillance cases.

3.5.4 Necessary in a Democratic Society – Margin of Appreciation

While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court.[111] A margin of appreciation is left to the competent national authorities in this assessment. In several cases, the Court has expressly recognised that "national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security".[112] As established in the previous chapter the Court's use of the margin stems from two sources: the subsidiary role of the Court and the level of deference built into the Convention. In this context the margin is stemming from the subsidiary role of the Court, as it acknowledges that national authorities are in a better position to judge the proportionality of their actions when it comes to national security matters.

The doctrine of a margin of appreciation in the context of secret surveillance cases stems from *Klass v Germany* where the Court stated that:

> As concerns the fixing of the conditions under which the system of surveillance is to be operational, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the

[108] *Soering v UK* (1989) 11 EHRR 439 para 89.
[109] *Sporrong and Lonnroth v. Sweden* (1983) 5 EHRR 35.
[110] Yutaka Arai-Takahashi, "The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR" (Antwerp: Intersentia, 2002), p 193.
[111] Ibid, para 49.
[112] *Klass and Others v. Germany* (1979) Series A no.28, Para 49, *Leander* para 59, and *Malone* para 81.

national authorities any other assessment of what might be the best policy in this field.[113]

The above quote outlines the subsidiary role the Court takes in matters concerning surveillance. While the quote implies a significant deference to the national authorities the Court acknowledged that this doesn't mean that "Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance".[114] The Court explained that unchecked surveillance regimes risk undermining or even destroying democracy under the cover of defending it and, as such, "Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[115]

This affirms the Article 10 *Handyside*[116] formulation in the context of Article 8 surveillance: that – while states do possess significant leeway in the schemes of secret surveillance which they choose to enact and enforce – this margin of appreciation is balanced by the power of the ECtHR as an international supervisory organ. However, Yourow argues that the record shows that the Strasbourg Court is "always prepared to approve such rights-restrictive state action as falling within the wide margin of appreciation which the states "enjoy" as an attribute of sovereignty, which Strasbourg recognises".[117] This is due to how the Court attempts to balance the interests of the State authority against the protection of individual rights. National security situations are historically, logically and intuitively "closest to the authority priority and furthest from the rights-protection priority".[118] By presenting their interest in order and security the State possesses a compelling interest justification for the Court who are sympathetic to the state interest. While the Court in *Klass* invoked fears of a police state and the danger of undermining or destroying democracy in the name of defending it, it nonetheless approved the surveillance regime on its face.[119]

Yourow argues this point further, using the case of *Leander v Sweden* to show how the margin of appreciation doctrine continues to serve the purposes of the state at the expense of

[113] *Klass and Others v. Germany* (1979) Series A no.28, Para 49.
[114] Ibid.
[115] Ibid.
[116] *Handyside v UK* (1979-80) 1 EHRR 737.
[117] Howard Charles Yourow,, *The margin of appreciation doctrine in the dynamics of European human rights jurisprudence* (Martinus Nijhoff Publishers 1996). p 52.
[118] Ibid.
[119] Ibid.

the rights of claimants. Another secret surveillance case, in *Leander* the Court again attempted to balance the "interest of the respondent State in protecting its national security … against the seriousness of the interference with the applicant's right to respect for his private life".[120] The applicant was dismissed from a temporary job as a naval museum technician because of an unfavourable governmental security check. The Swedish Personnel Control Ordinance made the applicant subject to security clearance, including secret police files checks. The applicant was refused a review of the dismissal decision, did not receive an explanation for his unfavourable appraisal and was denied an opportunity to respond to the police file contents by the Swedish Government. Yet, the Court found no breach of Article 8. Yourow uses this judgment as evidence that the *Leander* and *Klass* judgments "lie on a continuum in which the national security rationale continues to allow the Court to grant a wide margin of discretion to national authorities challenged by Article 8 privacy claims".[121] The Court is willing to grant the state a wide margin in determining the "pressing social need" standard which is at the heart of the necessity test:

> In these circumstances, the Court accepts that the margin of appreciation available to the respondent State in assessing the pressing social need in the present case, and in particular in choosing the means for achieving the legitimate aim of protecting national security, was a wide one.[122]

The Court has thus left the role of assessing the pressing social need, and the proportionality of the interference, within the State's margin of appreciation. So, for Yourow, the Court has abdicated its role in scrutinising the proportionality of rights-restrictive measures in this context. However, this is an overstatement. The Court performs its role through attaching significant weight to the presence of adequate safeguards. This can be found within *Leander* itself if one looks at the Court's implementation of the justifications test.

The Court first held that the aim of the legislation in question was clearly a legitimate one for the purposes of Article 8, namely the protection of national security. The main issues were then whether the interference was "in accordance with the law" and "necessary in a democratic society". The interference had a basis in domestic law and was clearly accessible in that it had been published in the Swedish Official Journal. Thus, the main question was

[120] *Leander v. Sweden* (1987) 9 EHRR 433, para 59.
[121] Howard Charles Yourow, *The margin of appreciation doctrine in the dynamics of European human rights jurisprudence* (Martinus Nijhoff Publishers 1996). p. 107.
[122] *Leander v. Sweden* (1987) 9 EHRR 433, para 59.

whether the domestic law laid down, with sufficient precision, the conditions under which the relevant authorities were empowered to store and release information under the system in question.

The Court's analysis of the first paragraph of the legislation found that the system conferred a wide discretion on the National Police Board as to what information can be entered in the register. However, this discretion was limited by law by the following paragraphs as well as the Swedish constitution, and by the fact that any entry of information into the register in question was subject to a necessity test and must have been in the pursuit of preventing or detecting "offences against national security etc". The legislation also contained explicit and detailed provisions as to what information may be handed out, the authorities to which information may be communicated, circumstances in which such communications may take place and the procedure to be followed when taking decisions to release information. Thus, the Court found that the Swedish law gave citizens adequate indication as to the scope and manner of exercise of the discretion conferred on the authorities in the system in question and the interference in the present case was therefore 'in accordance with the law'.[123]

The Court then proceeded to the 'necessary in a democratic society' test. The Court first stated that the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued. The Court then invoked the margin of appreciation in reframing the necessity test to one which balanced the interest of the respondent State in protecting its national security against the seriousness of the interference with the applicant's right to respect for his private life.[124]

The Court thus stated that the Government's margin of appreciation in assessing the pressing social need and, in particular, the means for achieving the pursued legitimate aim was in this instance a wide one. Nevertheless, given the risk that a system of secret surveillance runs the risk of destroying democracy on the ground of defending it, the Court held that there must exist adequate and effective guarantees against abuse. The Government then invoked twelve different safeguards which, in their opinion, constituted adequate protection when taken together. These included: parliamentary supervision, judicial supervision and the ability to

[123] Ibid paras 55 – 57.
[124] Ibid paras 58 – 59.

notify to the individual under surveillance although the Government admitted that this had never been used.[125]

In light of the wide margin of appreciation and the presence of adequate and effective guarantees against abuse, the Court found that the respondent State was entitled to consider that the interests of national security prevailed over the individual interests of the applicant. Thus, the interference in question could not be said to be disproportionate to the legitimate aim pursued. Returning to Yourow's argument then, in *Leander* the Court allowed the respondent State a wide margin of appreciation in determining that there was a pressing social need and that surveillance was a legitimate method of pursuing the stated aim. This effectively gave the state in question the go ahead to conduct surveillance. However, the Court placed significant weight on the presence of adequate safeguards against abuse in its ruling on the necessity test, showing that it was still trying to keep surveillance in check. It is the presence of safeguards that has been the lynchpin of the Court's judgments on the necessity of surveillance going forward.

3.6 Conclusion

There are a number of threads to follow through this exploration of the Court's approach to Article 8 and targeted surveillance case law in particular. These can be divided into two broad issues: (1) issues stemming from the covert nature of surveillance and (2) issues stemming from developments in technology.

3.6.1 Covert Nature of Surveillance

The establishment of victim status is very difficult in the context of surveillance. A state is not required to notify those who have been subject to covert surveillance, thus it is nearly impossible for an individual to gather evidence that they have been surveilled. This has led to a situation where the Court is willing to examine a potential interference of an individual's Article 8 rights due to the very existence of legislation allowing for surveillance. Although this only applies where there are no effective domestic remedies. Where such remedies exist, the applicants must show that they are potentially at risk of surveillance due to their personal circumstances. Two points follow from this: the tendency for the Court to view surveillance cases *in abstracto* and the question of what constitutes an effective domestic remedy.

[125] Ibid para 62.

The question of what constitutes an effective domestic remedy remains at large. In *Kennedy*, the Court ruled that the IPT was not an effective remedy due to it being unable to place a binding obligation upon the Government should it find legislation incompatible with the Convention. In *Big Brother Watch* the Court reversed this based on the fact that the Government had been willing to give effect to the IPT's findings voluntarily and that the IPT could appeal the ECJ in order to institute a binding obligation. Given that the UK will no longer be subject to the ECJ's binding obligations post-Brexit, this reliance on the discretion of one Government which is subject to change is insufficient.

In terms of the 'in accordance with the law' portion of the Court's approach, the Court takes a foreseeability orientated view of the test. Whether an interference has a basis in domestic law is rarely an issue and questions of accessibility are not raised. Combine this with the Court's tendency to stop its analysis of whether an interference is compatible once it has found a violation on the basis of foreseeability, and it becomes clear that foreseeability is carrying a lot of weight.

In terms of the legitimate aim portion of the approach the Court rarely questions a Government's assertion that it is pursuing the legitimate aim of protecting national security. This is because applicants never challenge this. Ordinarily in Article 8 cases this would not matter as the necessity test assesses whether an action is proportionate to the stated legitimate aim. However, as the Court's necessity test is hamstrung by the subsidiarity of the Court in the context of national security, this becomes an issue.

In terms of the necessity test, the subsidiarity of the Court in the context of national security has led to Governments being given a wide margin of appreciation in determining the pressing social need and the most effective means to address said need. While it has been argued that in doing so the Court has abandoned the question of necessity completely to the discretion of Governments this is not true. The tension between the Court's subsidiarity and its desire to provide effective protection of Convention rights has led it to create the adequate and effective safeguards against abuse test. While the margin of appreciation in this context is wide the Court will find Governments to be outside it if the legislation governing said interference does not contain adequate and effective safeguards against abuse. The exact content of these safeguards will be discussed in the chapter on bulk surveillance[126] but the fact that the Court simply checks whether these safeguards are present in the legislation

[126] See chapter 6 on 'Bulk Interception Caselaw of the ECHR'

places them firmly in the ‘in accordance with law’ test. This circles back to the question of the relative weight placed on the ‘in accordance with law’ test, and foreseeability in particular which will become an issue when less targeted forms of surveillance which are even more difficult to foresee come into play.

3.6.2 Developments in Technology

Since the first surveillance case, *Klass*, was decided in 1978 technological development has occurred at an exponential pace. This is true of both general technology and surveillance technology. In *Klass* the case concerned legislation pertaining to mail inspection, the recording of telephone conversations and telegraph interception. In 2018 the *Big Brother Watch* case concerned legislation pertaining to the bulk interception of millions of communications as they crossed transatlantic fibre optic cables. Thus, there are a large number of issues for the Court’s approach to attempt to encompass.

First, there is the interaction between the expectation of privacy and social media. The Court has relied on the expectation of privacy often in deciding whether an act of surveillance constituted an interference with Article 8. For example, the monitoring of a public place via CCTV does not constitute an interference. Questions arise however when this practice is translated online where the lines between public and private are necessarily blurrier. The Court has yet to rule on whether an openly available social media profile is a public and, if so, how to distinguish between public and private profiles. The varying functionalities of social media platforms complicates matters further. As discussed, Telegram channels are popular with political extremists, often infiltrated by law enforcement, journalists and academics, and constitute a private channel for thousands to congregate in. This is a near Gordian knot for the Court to eventually untangle.

Second, following on from the previous point, what private life considerations arise from the storage and aggregation of publicly available data? The Court has addressed this in cases like *Catt* and *Segerstedt-Wiberg* on the storage of political data. Social media companies by definition store the information entered on their platform and may share it upon request with Governments. How does this interact with the right to be forgotten, as once it has been shared with a government an individual has no recourse to have all instances of the data deleted. This interacts again with the covert nature of surveillance as the individual is very unlikely to be notified by either the social media company or government about the sharing of data.

Third, while it is relatively straightforward to determine whether an individual is a member of a group offline, this becomes murkier online. Returning to the Telegram example, while many members of extremist groups traffic in private channels, there are also academics, police and journalists present in these channels for research and counter-terrorism purposes. This presents an issue for the Court to address in future as individuals with no extremist affiliation may be subjected to surveillance. This is complicated further as journalists and academics who study violent jihadist groups may be Muslim themselves and at greater risk of negative consequences than their counterparts.

Fourth, while this thesis uses the examples of Facebook, Twitter, and Telegram as examples of contemporary social media platforms, it is likely that these will be outdated, or will have evolved, within a few years. Which platforms are used and the general functionality of social media platforms are subject to extensive change. This may lead to situations where the Court rules on one or two of the most popular platforms only for the world to have moved on by the time the Court passes judgment in the case In order to emphasise its effectiveness, the Court must commit to an ongoing evolutive interpretation of the technology in question.

These trends point to a larger trend that the Court's historic approach is not equipped for the demands of today both in terms of procedure and substantive principles. In terms of the covert nature of surveillance, there is a clear tension at play in the Court's approach between the Court's desire to provide meaningful protection to Article 8 rights and its subsidiary role to national legislatures. The Court's subsidiarity has led to Governments being given a wide margin of appreciation when deciding to utilise surveillance in pursuit of the legitimate aim of protecting national security. The Court has introduced the presence of adequate and effective safeguards against abuse test as a means of providing the most effective rights protection in the restrictive situation they find themselves in. However, this places a large amount of weight on the adequate and effective safeguards test which considering the rate of technological development may not adequately reflect the realities of bulk surveillance.

4. Understanding the Harms of Bulk Interception

This chapter aims to provide a full framework for both understanding how bulk interception works and its potential harms. To do so it first sets out a typology of terms to understand bulk surveillance more generally, in line with this the chapter sets out what data the act of bulk interception does and doesn't collect. The chapter next provides a technological explanation of how the UK bulk interception regime functions based on a comparison of official and unofficial sources. With this understanding in mind the chapter concludes by providing an analysis of the harms posed by bulk interception to privacy, freedom of expression and freedom of assembly. The scope of bulk interception and the harms posed by its use provides a uniquely difficult issue for human rights bodies such as the ECtHR and the CJEU to protect against, one which they may not be able to deal with.

4.1 Bulk Surveillance; a typology

It is useful here to define key terms. First, mass surveillance is an imprecise term which covers a multitude of surveillance apparatuses. It also carries multiple meanings and multiple subcategories. The framework this chapter builds concerns bulk surveillance which is more precise and has a basis in both UK national law[1] and international human rights law[2]. Murray and Fussey define the type of surveillance discussed in this chapter as Bulk Monitoring of Communications data in that it involves the large-scale collection, retention and subsequent analysis of communications data.[3] I find this to be a convincing, if simple definition as, like mass surveillance, bulk surveillance covers a number of different methods.

As of the writing of this chapter Bulk Surveillance can be divided into four distinct forms; interception, acquisition, equipment interference and personal datasets. These forms are derived from the UK Government's account of their surveillance operations. Bulk Interception is the most far reaching and covered form in terms of academic and journalistic sources. For clarity; Bulk Interception is the untargeted collection of online communications

[1] Investigatory Powers Act 2016 Part 6.
[2] *Weber and Saravia v Germany* (2008) 46 EHRR SE5, *Big Brother Watch and Others v. The United Kingdom,* App nos. 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018).
[3] Daragh Murray, and Pete Fussey. "Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data." (2019) 52 Israel Law Review 31-60. https://www.cambridge.org/core/journals/israel-law-review/article/bulk-surveillance-in-the-digital-age-rethinking-the-human-rights-law-approach-to-bulk-monitoring-of-communications-data/AA032EBA3EC3889D27054011853E5E59/core-reader.

as they cross particular bearers by surveillance apparatuses such as GCHQ. This definition will become clearer in the following section. Bulk acquisition is the untargeted collection of communications data from company private servers by request. Bulk equipment interference is the untargeted collection of data from devices through the implementation of hardware or software implants. Bulk personal datasets are large datasets of identifiable data derived from a multitude of sources.

Additionally, metadata is another broad term which I will avoid using in this chapter. Metadata can mean data about data, or the data about a communication or request that is not considered content data. It can be divided into descriptive, structural, administrative, reference and statistical metadata. In lieu of this imprecise term this chapter will focus on the term 'communications data'. Like bulk surveillance this term has a basis in both UK law and ECtHR jurisprudence. Under section 21(4) of the Regulation of the Investigatory Powers Act (RIPA) communications data is comprised of three subcategories; traffic data, service use information and subscriber information.

Traffic data is the primary data this chapter is concerned with. It consists of data "comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted".[4] As Bulk Interception concerns the collection of communications in transit, traffic data is the most applicable form of data to examine in this chapter. Service use information is more appropriate to examine in relation to Bulk Acquisition as it concerns "any information which is about the use made by the person" of any postal or telecommunications service. Subscriber information concerns anything not covered by traffic or service use categories that is held or obtained, in relations to persons to whom the service is provided. This form of information is more appropriately discussed in terms of Bulk acquisition or Bulk Personal dataset. Thus, going forward this chapter will explain the operation of bulk surveillance powers as they collect communication data.

4.2 Defining Metadata

Prior to outlining how each of the bulk powers operate, it is useful to drill down further into to the concepts of communications data and metadata. After the Snowden leaks a distinction was drawn between content and metadata. Content was seen as a protected form of

[4]Regulation of Investigatory Powers Act 2000 s21(4).

identifying data while metadata was seen as a resource which could be tapped into by security and intelligence such as GCHQ and the NSA. Metadata refers to the information gathered or processes as a consequence of a communication's transmission. Young states that this data can reveal the "latitude, longitude and altitude of the sender's or recipient's terminal, direction of travel … any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection".[5]

However, metadata is often conflated with 'communications data'. The UK Investigatory Powers Act 2016 for example relies upon the notion of communications data distinguished from the content of communications. The UK legislation attempts to breakdown in a systemic manner all the species of communications data without referring to the term "metadata". Metadata is often used as a shortcut to explain what communications data is within the meaning of the legal framework regulating law enforcement access to data retained by telecommunications operators or data retention obligations imposed upon telecommunications operators.[6]

Stalla-Bourdillon et al. break down the term metadata into three distinct categories; network-level, application level, and service use metadata.[7] The primary distinction made by the authors is between network and application level metadata. While network level metadata is first used to answer the question who speaks with whom, application level metadata "can directly reveal sensitive information such as political, religious or philosophical opinions or beliefs, as well as information concerning health or sex life."[8] Service use metadata stored by web or application servers can mirror both network and application level data.

It is important to distinguish between network level and application level in particular as the means by which an Internet Service Provider or operator can gather metadata on that level differs greatly. Capturing on the network level is relatively simple. A few lines of configuration on a network router that causes the required data to be sent to a collector device, which adds the data to a database that can later be queried for network analysis

[5] Jason M Young 'Surfing while Muslim: Privacy, freedom of expression and the unintended consequences of cybercrime legislation.' (2004) 7 Yale Journal of Law and Technology 346-421.
[6] Sophie Stalla-Bourdillon, Evangelia Papadaki, and Tim Chown. "Metadata, traffic data, communications data, service use information… What is the difference? Does the difference matter? An interdisciplinary view from the UK." In *Data Protection on the Move*, pp. 437-463. (Springer, Dordrecht, 2016).
[7] Ibid, p 4.
[8] Ibid.

purposes. By contrast the capturing of application-level metadata requires more detailed inspection of specifically the payload of the communication.[9]

The payload is the cargo of a data transmission. It is also known as the body or data of a packet. The payload contains the actual application content which in some cases may be encrypted, such as the text of the e-mail, website content etc. But it also contains application level metadata such as the subject line and sender and receiver e-mail addresses for an email or specific URLs for a web browser request. The process of inspecting these payloads is known as Deep Packet Inspection.[10]

Stalla-Bourdillon et al argue that the collection of application metadata should protected in the same way as the content of communications. They base this on the fact that the collection of said data requires the implementation of deep inspection technologies (such as DPI). Additionally, they argue said data can directly identify individuals, reveal sensitive information and be used to single out individuals and amount of profiling.[11]

If network and application level metadata can be said to be data captured in transit, service use metadata is captured at the end point, communication servers. A useful example of this form of metadata is an e-mail relay that is responsible for handling email for a given organisation. Typically, such a relay would be used to relay email messages in and out of the organisation, from clients within and outside of the organisation. In doing so the relay would log all transactions, noting such metadata as the sender's and recipient's email addresses, the date/time, the message size and the unique message-ID for the email. Generally, the content of the email sent through the relay is not stored. Generally, these logged summaries are used only to provide information on service use, such as the amount of emails sent and received in a given day or the proportion of emails which contained spam. But the collected metadata can also be used to identify a specific email stored somewhere through searching for the unique Message-ID. Another example is a web server that logs all accesses made to the server from user's web browsers, such as Google Analytics. While this data is usually used for technical troubleshooting, it can also be of great use for web-mining and traffic analysis. It can also be

[9] Ibid.
[10] Ibid p 8.
[11] Ibid p 20.

used to map individual web use if the IP addresses recorded in the logs are correlated between different web server logs and the user repeatedly uses the same IP address.[12]

It is easiest to explain the why application level metadata should be treated in the same manner as content data through comparative example. In this example I email my doctor concerning a private and embarrassing skin condition, the doctor responds and recommends a corresponding specialist. I then email this specialist, and in doing so all messages to and from me in this conversation cross a bearer targeted by GCHQ and are collected. If GCHQ are collecting metadata on the network level they see the following picture; one IP address communicated with another and upon receiving a communication from this address emailed a third. From the port number they could tell that this was through email and they could ascertain the size of the email and the duration of the communication. GCHQ would then run our IP addresses against their list of hard selectors and after finding that none were of intelligence value they would be automatically sifted out and deleted. Here bulk surveillance has achieved its goal while only inflicting a very limited privacy harm on me.

On the other hand, if GCHQ collected the communications metadata on the application level they would gain a lot more identifying information. As stated above, the collection of metadata on the application level involves the collection of the payload of the communication. The payload contains the content of the communication however GCHQ uses DPI to only examine the metadata. However, this metadata contains the subject line and email addresses involved in the communication. With this information it is easy to see that I am emailing my doctor and even if I did not refer to my embarrassing condition in the subject line the email addresses of the specialist would provide a large clue to this fact. If I emailed using my university affiliated email address then GCHQ knows that too. This information would go through the same process as the network level metadata and be automatically sifted out and deleted. However, this instance has achieved the same result by revealing a lot more identifying data about me and thus inflicting a greater privacy harm.

From this unpacking of the term metadata it is clear that the distinction made by the UK government in the Investigatory Powers Act is insufficient as it only draws a distinction between communications data and content data. In reality, communications (or metadata) can be divided into three levels; network, application and service level data. While network level

[12] Ibid p 9.

metadata does not enable the identification of particular individuals, application and service use metadata does. Thus, when the UK government states that content data should be protected from interference due to its identifying nature their logic necessarily extends to application and service use data. The identifying dichotomy between content and communications data is false as communications data can be just as, if not more, identifying as content data. From here we can derive that the collection of metadata is a privacy problem. Limiting collection of metadata does not mean that entities like GCHQ and the NSA are hamstrung in their security efforts. Network level metadata can be very revealing if used correctly. In 2013 a Harvard student, using the Tor browser to conceal his identity, emailed bomb threats to the school in order to avoid an exam. This provided him with a random IP address. He also used Guerrilla Email which gave him an anonymous, one time use email address. The FBI was able to identify him however because he had used the Harvard wireless network to connect to the internet.[13]

As can be seen above Stalla-Bourdhillon et al are keen to move the dividing line between content and communications data to include application level communications data in the protected zone along with content. However, it is unclear why the distinction should be kept at all. If the logic is that data which identifies individuals should be protected then there is no need for the distinction between the two broad categories of content and communications data. It may be more useful then to avoid this distinction between content and communications data in favour of a protection of identifying data similar to the distinction used in the EU General Data Protection Regulation (GDPR) for personal data. Under GDPR personal data means any information relating to an identified or identifiable natural person. Data which falls under this definition includes names, identification numbers, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In this manner a scale is provided wherein the more identifying a type of data is the more protections should be afforded to it.

Nonetheless, this more precise division of communications – or meta – data into application, service and network levels provides another means by which these powers can be differentiated in their operation. While the following outlines of each of the bulk surveillance

[13] Russell Brandom, 'FBI agents tracked Harvard bomb threats despite Tor' *The Verge* https://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor accessed 06/12/2021.

powers will focus on how they are used by SIAs (Security and Intelligence Agencies), it is important to note the differing forms of data which these powers collect. As different types of data can be more or less identifying, the intrusiveness of the powers which collect them is inherently tied to the data they collect. This chapter will avoid the use of terms such as mass surveillance or metadata except for when it is necessary to realise a point or cite another work.

4.3 Bulk Interception

Interception can be described as a process where communications are collected in the course of transit, such that the content becomes available to someone other than the sender or recipient. The main focus of the examination of the intercepted communication must be overseas (foreign focused).[14] Bulk interception is the same basic process as this but typically involves the collecting of communications as they transit particular bearers (communication links). This process is divided into three stages; collection, filtering, and selection for examination.

In Lord Anderson's Report of the Bulk Powers Review 2016 it is described as a capability

designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and analyse that material in order to identify communications of intelligence value.[15]

It is exercised under the bulk interception warrants provided for under sections 136 to 142 of the Investigatory Powers Act 2016.[16] Bulk interception is only carried out by GCHQ.

In the case of bulk interception it is often pointed out that human eyes do not see the communications until the third stage, selection for examination, as an argument for a lesser intrusion on Article 8 rights.[17] However, this argument raises several key concerns about the process, specifically the presence or lack thereof of human oversight in the process. As mentioned in chapter 1, if the only human presence in the collection stage is the selection of the specific bearer to be tapped, then it is unclear how GCHQ knows that that specific bearer

[14] Investigatory Powers Act 2016, s 129(2).
[15] David Anderson QC, *Report of the Bulk Powers Review* (2016) p 21.
[16] Investigatory Powers Act 2016, s 136 (6)(1).
[17] See chapter 4 on "Understanding the Harms of Bulk Interception".

is of intelligence value.[18] The plausible answer to this is that the bearer is tapped and the justification of having intelligence value is applied to the bearer retroactively once they have found such communication in the third stage. Second, it is unclear how the information is filtered via algorithm. Again, as discussed in chapter 1, the algorithm works off a list of selectors of varying specificity. These selectors include certain terms and email addresses but are not publicly available owing to the covert nature of surveillance. As discussed later in this chapter officials are given access to the filtering system in order to check that it is working.

Prof Ian Brown of the Oxford Internet Institute provided expert testimony for the Privacy NGO Big Brother Watch in their application to the European Court of Human Rights. In his testimony he provides a useful diagram, below, to explain how bulk interception may work. This diagram is informed by his knowledge of technology and his reading of the Snowden leaks. It concerns the collection of an email between an individual located in Germany and an individual in the UK. Each of the stages of Bulk interception in the diagram is denoted by a number.

[18] Ibid.

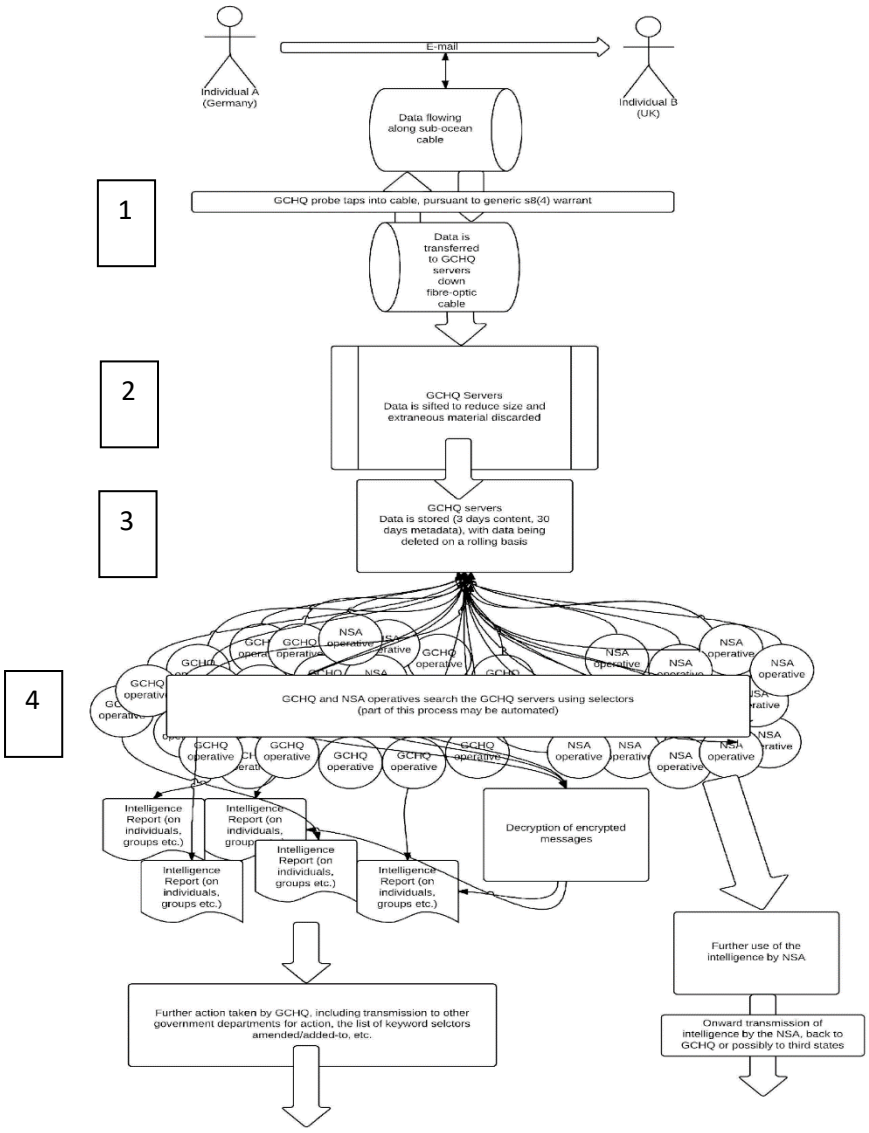

Figure 1. Bulk Interception Process Diagram

At stage one this email passes through under-sea cables via US servers. As the email passes through the tapped cable it is collected and sent to GCHQ's servers. At stage two it is automatically buffered along with a large amount of other data in order to reduce the size of the collected data and to exclude irrelevant captures. The data which survives this automatic filtering process is then stored at stage three wherein content data is stored for a much shorter period than metadata; three days for content compared to 30 days for communications data. This data is deleted on a rolling basis meaning that as new data is collected old data is deleted. During this window of time that data then may be picked up through the use of keyword/indicator searches, such as XKEYSCORE. GCHQ operatives then use the content to compile intelligence reports which are then transmitted elsewhere for further action. It is probable that such a communication would then be stored, or a copy made, before the content

data that it was 'buffered' alongside is deleted. The communications data would, it appears, be available to be searched for a longer period before being deleted. This data could then be used by the US authorities.[19] These four stages provide a useful structure for this chapter and each will be examined more thoroughly in their respective section.

This section aims to provide a clear picture of how communications are collected in the first stage of Bulk Interception. This picture is currently unclear due to conflicts between official and unofficial sources. There are two narratives on the technological capacities of the UK government to carry out bulk interception of communications and this can be seen immediately in stage one. The government's official statements describe targeted interception as the collection of communications in the course of transit, such that the content and communications data becomes available to someone other than the sender or recipient. Bulk interception is the same basic process as this but typically involves the collecting of communications as they transit particular bearers (communication links). Avoiding the label of mass surveillance *"*GCHQ selects which bearers to access based on an assessment of the likely intelligence value of the communications they are carrying*"* [20.] The *Report of the Bulk Powers* review points out that GCHQ has neither the capacity nor the legal authority to access every bearer in the world; "At any given time, GCHQ has access to only a tiny fraction of all the bearers in the world*"*[21], and so focuses its resources on links which they assess will be most valuable.

This narrative seems at odds, in part, with the narrative derived from the Snowden leaks. As per the 2013 Snowden leaks, the main form of bulk interception of communication and content data in the UK comes from the Tempora Programme. It should be noted that the UK government has neither confirmed nor denied the existence of this programme.[22] Under Tempora GCHQ has placed data interceptors on fibre-optic cables conveying Internet data in and out of the UK. These UK-based fibre-optic cables include transatlantic cables between the US and Europe, and it is believed that interceptors have been placed on at least 200 "wavelengths" (data channels) carried by fibre optic cables, near to the points where they come ashore. This appears to have been done with the secret co-operation of the companies

[19] Ian Brown, Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK (September 27, 2013). Application No: 58170/13 to the European Court of Human Rights. Available at SSRN: https://ssrn.com/abstract=2336609.
[20] David Anderson Q.C. 'Report of the Bulk Power Review' (2016) p 23.
[21] Ibid.
[22] ibid p. 79.

that operate the cables. The programme is reported by *The Guardian* to have been operational since 2011.[23]

The importance of these cables cannot be overstated as they form the main arteries of the Internet worldwide. If they can be successfully tapped, then they provide a 'fast track' to total Internet surveillance, without the need to target an individual user with more specialised surveillance methods.[24] The cables located in the UK are of particular importance as they are the landing point for the majority of transatlantic fibre-optic cables. This means that monitoring of these cables will cause a large quantity of communications relating to the rest of the world will be caught. Much of the rest of Europe's external internet traffic is routed through the UK.[25]

An unnamed intelligence source stated to *The Guardian* that *"*There is no intention in this whole programme to use it for looking at UK domestic traffic – British people talking to each other"[26]. However, it is clearly within GCHQ's capabilities to do so. Additionally there is no suggestion in the source materials reported by *The Guardian* that 'purely domestic' traffic was being excluded under the Tempora programme.[27]

Ian Brown speculates as to how GCHQ is tapping these cables in his expert's opinion for the *Big Brother Watch v UK* case. It is most likely done through the use of an 'optical splitter', which duplicates the light signals flowing through the cables. He expects that these duplicated signals are transported over further fibre optic cables to GCHQ's storage and processing centres in Bude, Cheltenham and elsewhere.[28] *The Guardian* reported that "by summer of 2011, GCHQ had probes attached to more than 200 internet links, each carrying data at 10 gigabits a second"[29]. Brown expects that the location of the tapping is likely where the cables make landfall. Additionally *The Guardian* reported that the tapping had been carried out in cooperation with the companies who own the cables, reporting that "companies have been paid for the cost of their co-operation and GCHQ went to great lengths to keep

[23]*GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, 21 June 2013 [https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa]
[24]Ian Brown, Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK (September 27, 2013). Application No: 58170/13 to the European Court of Human Rights. Available at SSRN: https://ssrn.com/abstract=2336609.
[25] Ibid.
[26] Ewan MacAskill and others, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian* https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[27] Ibid.
[28] Ibid.
[29] Ibid.

their names secret. They were assigned "sensitive relationship teams" and staff were urged in one internal guidance paper to disguise the origin of "special source" material in their reports for fear that the role of the companies as intercept partners would cause "high level political fallout"[30].

Cayford et al[31] agree that wiretaps on fiber-optic cables are likely the means by which the NSA accesses and captures vast amounts of data. They base this assertion on three points. First, according to an NSA slide[32], from the Snowden leaks, "Upstream" is "the collection of communications on fiber cables and infrastructure as data flows past."

Second, TEMPORA is known to be tapping into fiber-optic cables and to be working with the following telecom companies; BT, Verizon Business, Vodafone Cable, Global Crossing, Level 3, Viatel, and Interoute.[33] In 2013 *The Guardian* reported that a German paper, *Suddeutsche* had published the names of the commercial companies working secretly with GCHQ. The specific document cited is from an internal GCHQ powerpoint presentation from 2009 discussing TEMPORA. The slides in question outlined the top secret codenames for each firm; BT ("Remedy"), Verizon Business ("Dacron"), Vodafone Cable ("Gerontic"), Global Crossing ("Pinnage"), Level 3 ("Little"), Viatel ("Vitreous") and Interoute ("Streetcar").[34] Together these seven companies control a huge share of undersea fibre optic cables necessary for the internet to function and the fact that they were working with GCHQ lends credence to Cayford et al's theory that wiretaps are the primary method of bulk interception.

Finally, a 2006 court case against AT&T, which disclosed that the NSA was wire-tapping fiber-optic cables at AT&T's internet exchange point in San Francisco.[35] Specifically a veteran AT&T technician released documents in testimony that described equipment capable of monitoring a large quantity of e-mail messages, Internet phone calls, and other internet

---

[30] Ibid.

[31] Michelle Cayford, Coen Van Gulijk and Pieter Van Gelder, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014).

[32] Slide no. 3 of the NSA presentation: Working principle of Upstream and PRISM. (FAA702 Operations. Two Types of Collection. NSA, 2013.

[33]James Ball, Luke Harding, & Juliette Garside. "BT and Vodafone among Telecoms Companies Passing Details to GCHQ." The Guardian, August 2, 2013. https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

[34] Ibid.

[35] John Markoff and Scott Shane, "Documents Show Link Between AT&T and Agency in Eavesdropping Case" The New York Times, April 13, 2006 https://www.nytimes.com/2006/04/13/us/nationalspecial3/13nsa.html..

traffic. The technician claimed that this equipment was installed by AT&T in 2003 and was able to select messages that could be identified by keywords, email addresses, country of origin and IP address, and divert copies to another location for further analysis.

The Guardian reported that this mode of surveillance potentially gives GCHQ access to 21 petabytes of data a day. A petabyte being approximately 1000 terabytes, which is in turn 1000 gigabytes. The commonly used example for scale is that the data GCHQ has access to is equivalent to sending all the information in all the books in the British library 192 times every 24 hours.[36] The Tempora programme gives GCHQ the largest internet access out of the "Five Eyes" group (Australia, New Zealand, Canada, USA, UK).[37]

Given that this form of surveillance provides 21 petabytes of data each day, it is necessary that agencies such as GCHQ or the NSA filter this data in order to find valuable information. Under the Tempora programme, both metadata and content data are sifted using a two stage technique called Massive Volume Reduction (MVR). An example of what is sifted out through MVR in the first stage is peer-to-peer downloads of music, films and computer programmes. These are classed as "high volume, low value traffic" and accordingly filtered out, reducing the volume of data by 30%.[38] This is backed up by official releases on the topic such as the code of practice for the Bulk Surveillance programme which states that a degree of filtering is applied to the traffic to the data extracted from communications links and signals. This filtering process is designed to select types of communications of potential intelligence value whilst discarding those least likely to be of intelligence value. Interestingly here the official description blurs the line between filtering and the next step we will discuss, selection for examination. It does this by stating that further complex searches may then take place to draw out further communications most likely to be of greatest intelligence value. These communications may then be selected for examination. However, as I will argue in the following section, these complex searches are not filtering but an integral part of selection for examination. Given that all of the powers outlined here have a selection for examination process, this section will follow the descriptions of the bulk powers.

---

[36] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "How does GCHQ's internet surveillance work?" The Guardian, June 21, 2013 https://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

[37] Ibid.

[38] Ian Brown, Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK (September 27, 2013). Application No: 58170/13 to the European Court of Human Rights. Available at SSRN: https://ssrn.com/abstract=2336609 para. 32.

4.4 Selection for Examination

While this section aims to provide a clear picture of how the examination of collected data works for each of the bulk powers, it is limited by the official sources. In the official sources there is only a clear explanation of the selection for examination for bulk interception. While there are mentions of selection for examination processes for each power in their codes of practices, only Anderson's Review of the Bulk Powers provides a clear account of bulk interception examination processes.

Following collection and filtering the remaining data is then searched using selectors. These include keywords, email or other address of interest, or the known names or aliases of targeted persons, and phone numbers. As of the 2013 leaks *The Guardian* reported that GCHQ and the NSA have respectively identified 40,000 and 31,000 such selectors. Brown anticipates that such sifting is partly automated, with an ever-expanding list of keywords and selectors being added to the list that is searched. It is unclear, however, when a log will be created – whether it is when information is read by searcher, or whether it is when useful information is found by a searcher – but in either case, it is likely that the logs may not provide a complete picture of the searching activities and the surveillance carried out. There are two reasons for this, that automated analysis of large quantities of data without human intervention are less carefully audited, and the reported use of the NSA's XKEYSCORE programme by GCHQ.[39]

Here it is again useful to point out the two differing narratives of how this surveillance is carried out. One narrative will be drawn from more official sources, such as Anderson's Review of the Bulk Powers and UK court submissions to the ECtHR while the other will draw from the Snowden leaks and surrounding literature. Following this, similarities will be outlined in order to paint a clearer picture of this process.

From the Snowden leaks it is easy to describe how XKEYSCORE operates, Cayford et al provide a useful description of the program.[40] Under XKEYSCORE GCHQ can undertake broad categories of searches through captured data in a process akin to using standard Internet search engines. Specifically, it processes data by running plug-ins, analysis engines

[39] Ibid.

[40] Michelle Cayford, Coen Van Gulijk and Pieter Van Gelder, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014).

that look for specific content in the captured data packets. These plug-ins for email addresses, phone numbers, webmail and chat activity, and extracted files amongst others. Said plug-ins extract the metadata from each internet session and index it into tables, this data can then be tracked, cross-indexed and searched for.[41]

There are approximately 150 XKEYSCORE sites around the world which include wiretaps at telecommunication companies peering sites, systems connected to friendly foreign intelligence agencies' collections and mid-ocean fiber-optic cable taps. While only information that is related to specific cases is sent back to the NSA's central database, data in the local caches is available to analysts through federated search while it is being stored.

To perform a search request an NSA analyst creates a query. This query is sent to all the XKEYSCORE sites. Analysts can search by hard selectors (email addresses) or soft selectors (language). So if an analyst doesn't have a hard selector, such as an email address or phone number for a known target, he/she can do a search for a category of information, such as all encrypted Word documents or all VPN startups in a given country (NSA XKEYSCORE slides 2008). Any kind of query can be created as long as the plugin exists. The program combines and returns all the responses to the query.

Using this programme is apparently how the NSA can identify Tor users – this is a category that can be queried. Another category that can be searched is exploitable machines in any country. "Show me all exploitable machines in country X" (NSA XKEYSCORE slides 2008). When the NSA's Tailored Access Operations (TAO) identifies a computer as a target it loads its fingerprints, or unique identifiers, into XKEYSCORE's fingerprint ID engine. In the case of Microsoft system crashes XKEYSCORE identifies these error reports and sends an automatic notification, enabling TAO to exploit the machine.[42]

XKEYSCORE performs best when it 'goes shallow' that is, fewer filters are applied to determine which data packets are captured. This means that a lot of information is collected, including, undoubtedly, information unrelated to NSA or GCHQ targets. XKEYSCORE, therefore, classifies as mass surveillance technology. In terms of manpower *The Guardian* reported that GCHQ has 300 operatives tasked with sifting through collected data in

[41] ibid. p 648.
[42] Staff. "Inside TAO: Documents Reveal Top NSA Hacking Unit." Spiegel Online, December 29, 2013. http://www.spiegel.de/international/world/the-nsa-uses-powerfultoolbox-in-effort-to-spy-on-global-networks-a940969.html.

partnership with 250 NSA operatives.[43] The numbers of people who subsequently have access to data are no doubt much larger as NSA access to GCHQ data is substantial.

The official review is drawn from the then Independent Reviewer of Terrorism Legislation David Anderson Q.C.'s Report of the Bulk Powers Review. As per Anderson's review[44], following the filtering remaining communications are then subjected to the application of queries to draw out communications of intelligence value. Two processes typically occur in this stage, a 'strong selector' process, and the 'complex query' process.

The 'strong selector' process operates on the bearers that GCHQ has chosen to access in step 1. As the internet traffic flows between those bearers, the system compares the communication against a list of strong selectors in near real-time. These strong selectors include specific telephone numbers or email addresses. Any communications which match the selectors are automatically collected and all the others are automatically discarded. Anderson notes that due to the global nature of the internet the route a particular communication will take cannot be predicted and a single communication is broken down into packets which can take different routes. GCHQ's processing system relies on accessing the 'related communications data' in the bearer to identify and reconstruct the wanted communications of subjects of intelligence interest. In order to apply these strong selectors all communications on a bearer has to be held for a short period. Legal opinion on whether this requires a targeted or a bulk warrant is split. Under the current UK Investigatory Powers Act this requires a bulk warrant. However, in the opinion of the Intelligence and Security Committee of Parliament (ISC); "while this process has been described as bulk interception because of the numbers of communications it covers, it is nevertheless targeted since the selectors used related to individual targets."[45]

The "complex query" process operates on a far smaller selection of bearers than its strong selector counterpart and is used where GCHQ is looking to match much more complicated criteria which may include weaker selectors but which in combination aim to reduce the odds of a false positive. The bearers examined are chosen for their likeliness to provide communications of intelligence value. This process is closer to the textbook definition of bulk interception outlined above as it involves the collection of *"unselected content and/or*

[43] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball. "GCHQ taps fibre-optic cables for secret access to world's communications" (2013) The Guardian.
[44] David Anderson Q.C., *Report of the Bulk Powers Review* (2016).
[45] ibid, p 24.

secondary data"[46]. It permits types of analysis and selection that are not currently achievable in the strong selector process due to its near real-time environment. Similarly to this first process any communications unlikely to be of intelligence value are discarded as soon as that becomes apparent.

The ISC, in their March 2015 report reject any allegations that this process is of untargeted of blanket surveillance as "this interception process does not therefore collect communications indiscriminately" and "only the communications of suspected criminals or national security targets are deliberately selected for examination."[47] The Independent Terrorism Reviewer found no reason to disagree with these statements though admitted that they had no scope with their review to conduct a detailed examination of GCHQ's selection and examination processes.

In contrast to the earlier narrative contrast the two narratives at play here are more complementary than not, with each shedding light on the other. If we take the Strong Selector process of the official narrative where the system compares the communication against a list of strong selectors in near real-time as it transits the tapped bearers. The bearers in question may well be, at least in part, those 150 XKEYSCORE sites.

The 'hard selector/soft selector' of the XKEYSCORE system and the 'strong selector/complex query' of the official narrative line up both in name and in practice. In both strong selector processes the system searches by selectors such as email addresses, names, phone numbers, specific file names etc. In the official narrative this search requires all communications on a bearer have to be held for a short time in order for the selectors to be applied. XKEYSCORE uses plug-ins to search cached data collected from the interception.

The 'complex query' process is by the reviewer's own admission closer to the textbook definition of bulk interception as it involves the collection of unselected content and/or secondary data. This data is drawn from a far smaller selection of bearers than its strong selector counterpart. Weaker selectors are then applied in order to reduce the likelihood of a false positive. XKEYSCORE provides an example of these weaker selectors in the form of searching for categories. These include all encrypted word documents or all VPN start-ups within the country.

[46]ibid, p 25.
[47]Ibid.

Another form of analysis disclosed in the Snowden Leaks is the KARMA POLICE programme. This programme "aims to correlate every user visible to passive SIGINT with every website they visit"[48]. The two products of this analysis are (a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet. One documented use of KARMA POLICE concerns the monitoring of internet radio stations to spread radical Islamic ideas. A GCHQ unit known as the Network Analysis Center compiled a list of the most popular stations, the majority of which had no association with Islam. They then zeroed in on any stations broadcasting recitations from the Quran. They then used KARMA POLICE to find out more information of these stations' listeners, identifying them as users on Skype, Yahoo, and Facebook. One Egypt based listener was then selected for profiling and GCHQ investigated what other websites he had been visiting. This revealed that the listener had viewed Facebook, Yahoo, YouTube, Blogspot, Flickr, a website about Islam, an Arab advertising site and the porn site Redtube.[49] What is clear from these analyses of the bulk interception process is that it is possible for a huge amount of data to be collected, filtered and examined in order to make clear, intrusive, profiles of individuals' behaviour and identities which can be aggregated into large searchable database. However, it is necessary to extrapolate the actual harms of the operation of bulk interception.

4.5 Harms of Bulk Interception

4.5.1 Privacy

The most obvious harm to the individual stemming from the use of bulk interception is the harm to privacy. Macnish emphasises the need to define what privacy means in a post-Snowden world. Specifically, whether privacy is a matter of control or access. The control definition is the argument that a loss of control over one's information constitutes a loss of privacy. To Inness privacy is defined as "a variety of freedom, a freedom that functions by granting the individual control over the division between the public and the private with respect to certain aspects of her life."[50] The access definition is the argument that the loss of privacy only occurs when one's information is actually accessed. Mcnish argues that the access account is correct. They give the example of leaving your personal diary in a café.

[48]The Intercept, 'Pull Through Steering Group Minutes' (*The Intercept,* 25/09/2015) <https://theintercept.com/document/2015/09/25/pull-steering-group-minutes/> accessed 09/06/2022.
[49] Ryan Gallagher "Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities" The Intercept September 25, 2015 https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.
[50] Julie Innes, *Privacy, Intimacy, and Isolation* (Oxford: Oxford University Press, 1992), p. 42.

Upon your return you find the diary in possession of a stranger who informs you that they have not read it, as they were only keeping it safe for your return. In Macnish's view their privacy has not been harmed by this incident despite the diary not being within their control. By extension, if the government collects but does not access your personal information then there is no privacy violation. Importantly, Macnish sees the collection of the data as a greater magnitude than a mere privacy violation.[51] Rather the collection of data entails harm to the rights that privacy protects. By focusing the argument against the use of bulk surveillance practices on privacy it may be harder to persuade the supporters of GCHQ's actions of their true harm. Here Macnish highlights the main justification of bulk surveillance used by GCHQ, that they are not violating people's privacy except in specific, justifiable, targeted cases. To Macnish this true harm is the chilling effect that one may feel if they believe that the state has collected their information and may access it at their will. This will be further discussed in the following section on freedom of expression.[52]

The most common response to the violation of privacy argument against bulk surveillance is the 'nothing to hide' argument. That when the government gathers or analyses personal information many people declare that they have nothing to hide. Therefore, the privacy interest is generally minimal and its contest with security is a losing one. The nothing-to-hide argument focuses just on one or two particular kinds of privacy problems: the disclosure of personal information or surveillance. This argument allows for the justification of a national security surveillance program that demands access to personal information. Either there is no problem at all with this program, because there is nothing to hide, or the benefits of the program far outweigh the harms to privacy. The first justification influences the second, because the low value given to privacy is based on a narrow view of the problem. Solove argues that even privacy advocates base their arguments against surveillance on the same premises as the nothing-to-hide argument.[53] For example, Bartow's claim that in order for privacy problems to have real resonance they must "negatively impact the lives of living breathing human beings beyond simply provoking feelings of unease".[54] This objection is consistent with the nothing-to-hide argument as those advancing this argument nothing-to-hide have in mind a particular kind of appalling privacy harm, where privacy is violated only

[51] Kevin Macnish, 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World' (2018) 35 Journal of Applied Philosophy 2.
[52] Ibid.
[53] Daniel Solove 'Why privacy matters even if you have nothing to hide.' (2011) Chronicle of Higher Education 15
[54] Ann Bartow, 'A feeling of unease about privacy law.' (2006) 154 U. PA. L. Rev. 477

when some kind of deeply embarrassing or discrediting information is revealed. To Solove a better understanding of the threat to privacy posed by surveillance is erosion over time, where privacy is threatened more by the slow accretion of a series of relatively minor acts rather than a single egregious act.[55]

Richards provides a strong argument as to the dangers of surveillance in the post Snowden revelations world. For Richards there are two points at which surveillance is particularly harmful. First is when the act of surveillance chills our exercise of our civil liberties.[56] Specifically, he refers to the harm to what he terms "intellectual privacy". This term refers to the theory that new ideas often develop best away from the intense scrutiny of public exposure, that people should be able to make up their minds at times and places of their own choosing and that a meaningful degree of privacy is necessary to promote this kind of intellectual freedom. When we are watched while engaging in intellectual activities such as reading, web surfing or private communication, we are deterred from engaging in thoughts or deeds that others might find deviant.[57] Richard's draws on Bentham's panopticon here wherein a prison is designed with a central surveillance tower from which a warden could see into all of the cells. In this situation, the prisoners had to conform their activities to those desired by the prison staff because they had no idea whether they were being watched at any given time.[58]

Second is the effect surveillance has on the power dynamic between the watcher and the watched, as it gives the watcher greater power to influence or direct the subject of surveillance. This could be for purposes as explicitly harmful as blackmail, Richards highlights the attempts by the FBI to blackmail Martin Luther King Jr. While the FBI's surveillance took a lot of effort in the 1960s, wiretapping his phones as well as his advisors' phones, hiding microphones in his hotel rooms, the same level of surveillance could be carried out with relatively little effort in 2023. A government or political opponent could obtain not just access to his telephone conversations, but also his reading habits, emails, and internet search history.[59] This is a harm both in authoritarian societies and democratic societies, surveillance often detects crimes or embarrassing activities beyond and unrelated to

[55] Daniel Solove 'Why privacy matters even if you have nothing to hide.' (2011) Chronicle of Higher Education 15
[56] Neil Richards, 'The Dangers of Surveillance' (2012) 126 Harv L Rev 1934.
[57] Neil Richards, 'Intellectual Privacy' (2008) 87 Tex L Rev 387.
[58] Neil Richards, 'The Dangers of Surveillance' (2012) 126 Harv L Rev 1934 p 1948.
[59] Ibid p 1955.

its original purposes. The surveillance of Martin Luther King Jr discovered evidence of his marital infidelity which was then used to blackmail him. Whether these discoveries are important, incidental, or irrelevant, all of them give greater power to the watcher.[60]

The harms of this intrusion on privacy are not limited to blackmail however, the act of surveillance also allows the watcher an increased ability to persuade or influence the watched. Governments use the power of surveillance to control behaviour, the predominant example being closed circuit television (CCTV) networks in modern urban areas. These networks allow police greater ability to watch and influence what happens in these areas. This may include persuade citizens to obey the law but may have other effects as well such as discouraging protest and encouraging public behaviour towards commerce.[61] Another possible harm stemming from surveillance is that it provides the ability to sort and discriminate between people based on private information and data.[62]

4.5.2 Freedom of Expression

The harm of bulk interception on freedom of expression stems from the idea that certain state actions may chill or deter people from exercising their freedoms or engaging in legal activities. There are a number of theoretical approaches to this chilling effect.[63] The first theoretical exploration of this concept comes from Schauer's work. In Schauer's theory government surveillance may chill or deter people from engaging in legal activities because they fear legal punishment or criminal sanction and do not trust the legal system to protect their innocence.[64] Solove's work has applied this theoretical approach to modern surveillance and big data gathering, arguing that these practices create a kind of regulatory environmental pollution that encourages chilling effects and self-censorship.[65] While Solove doesn't discount Schauer's reasons for the chilling effect he adds that these acts enhance the risk that a person may suffer harms in the future, such as data gathering about a person's activities may increase the risk the risk that they may be later subject to identity theft or fraud. In this view a person may avoid certain legal activities, not because they fear actual punishment but

[60] Ibid.
[61] Ibid p 1934.
[62] Ibid.
[63] Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2017) 31 Berkeley Technology Law Journal 118.
[64] Frederick Schauer, 'Fear, Risk, and the First Amendment: Unravelling the "Chilling Effect"' (1978) 58 BU L REV 685.
[65] Daniel Solove, 'A Taxonomy of Privacy' (2006) 154 U. PENN. L. REV 477

because they want to avoid other kinds of risk. These can include the stigma of being labelled or tracked by state authorities, being labelled as a non-conformist, deviant or criminal, or the broader concern that the information gathered about the activities will be leaked to the public.[66]

Penney's study examined how traffic to privacy sensitive Wikipedia article reduced following the Snowden revelations. The study examined 48 Wikipedia articles that corresponded with the DHS keywords listed as relating to terrorism, including "dirty bomb," "suicide attack," "nuclear enrichment," and "eco-terrorism"). The study found sudden, large, and statistically significant drop during and after June 2013 for terrorism related Wikipedia articles. Stoycheff examined the Facebook activities of Americans in the aftermath of the Snowden revelations. Her study found that "knowing one's online activities are subject to government interception and believing these surveillance practices are necessary for national security play important roles in influencing conformist behaviour."[67] In a later work Stoycheff examined the use of website cookies by participants who had been informed that they may be subjected to government surveillance for national security purposes.[68] Wicker and Ghosh's work on the impact of surveillance technology in ebooks shows this potential chilling effect: "to explore Marxism, sexuality, or addiction on one's Kindle one must allow Amazon to not only know that we may read the given material, but to know when, where, how much and with which fellow Kindle consumers one is reading the material."[69]

Buchi et al's work on the chilling impact of what they term "digital dataveillance" is invaluable to this analysis. To Buchi et al, digital dataveillance is "the automated, continuous, and unspecific collection, retention and analysis of digital traces by state and corporate actors."[70] They place this chilling effect in a system level context where dataveillance practices on the system level incur a sense of dataveillance on the individual level, defined as a feeling of being subjected to dataveillance and beliefs about dataveillance practices. This in turn leads to inhibited digital communication behaviour through the impact of the chilling

[66] Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2017) 31 Berkeley Technology Law Journal 118.
[67] Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) 93 Journalism and Mass Communication Quarterly 296.
[68] Elizabeth Stoycheff, 'Cookies and content moderation: affective chilling effects of internet surveillance and censorship ' (2023) 20 Journal of Information Technology & Politics 113.
[69] Stephen B Wicker and Dipayan Ghosh, 'Reading in the Panopticon - Your Kindle May Be Spying on You, But You Cannot Be Sure' (2020) 63 Communications of the ACM 68.
[70] Moritz Buchi, Noemi Festic and Michael Latzer, 'The chilling effects of digital dataveillance: a theoretical model and an empirical research agenda' (2022) 9 Big Data & Society 1.

effect. This inhibited individual level behaviour has societal impacts on the system level in terms of democratic quality, well being and trust, which in turn effects governance in terms of steering by the state, industry, markets and users. Finally, these changes in governance leads to increased dataveillance practices which begins the cycle all over again.[71]

The work of Stevens et al provides a well needed case study of the impacts of these broad surveillance practices. Drawing on interview data from participants subjected to state sponsored surveillance in Zimbabwe the study emphasises the varying chilling effects at play from this integrated ensemble of surveillance practices. Changes to individual behaviour reported by the participants included increased restraint in political conversations, eroded interpersonal trust, increased self-censorship, limited participation on social media and restricted access to work and economic activity due to blacklisting. In terms of freedom of expression one participant noted that they "always practice what I would call 'self-censorship' … I carefully construe how I communicate on certain issues and discuss them in a way that does not provide an opportunity for surveillance to become actionable."[72]

4.5.3 Freedom of Assembly

In his attempt to restructure the debate around the harms of surveillance Paul Bernal provides an analysis of the impact of bulk surveillance on freedom of assembly and association. The internet provides previously unimaginable tools for groups, assemblies and associations of all kinds. Groups founded purely through online services such as social media, forums and messaging apps have had real world impact. However, the online aspect of this organisation makes it particularly vulnerable to state efforts at internet surveillance. Bernal cites the efforts of the Tunisian state to hack in both Facebook and Twitter to attempt to monitor the activities of potential rebels but also the efforts of UK authorities to monitor social media during a riot or peaceful protest and to examine the social media activity of those organising the protests.[73] Bernal points out that it is easy to make a decision on an extreme case, such as in the case of a riot, but there are grey areas and the temptation for authorities to use tools once they are in place can be hard to resist.[74]

---

[71] Ibid.
[72] Amy Stevens, Pete Fussey and Otto Saki, ''I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe' (2023) 10 Big Data & Society 1.
[73] Paul Bernal, 'Data gathering, surveillance and human rights: recasting the debate' (2016) 1 Journal of Cyber Policy 243.
[74] Ibid.

In line with this Siatitsa analyses how digital technologies have significantly expanded the capabilities of authorities to surveillance assemblies: "Technologies are used to monitor the planning and organisation of protests, conduct surveillance during protests and even to continue surveillance after protests."[75] With each new protest the list of surveillance capabilities grows longer. Authorities have the ability to monitor social media communications and collect all information posted in relation to the protest indiscriminately, and this only intensifies during the act of protest where surveillance technology can be used to set up fake mobile phone towers, facial recognition software, sentiment analysis software and the use of military drones to ensure that no protester is able to remain anonymous if the authorities so wish it.[76] Ulrich and Wollinger detail how drones have been used by German police to monitor political protests.[77] Aston's work conducted interviews with thirty-five people who had direct experience of being the subject of overt police surveillance at political meetings, demonstrations, rallies and other forms of protest and compared their experience with the view of the UK courts on the impact of said surveillance.[78]

4.6 Conclusion: A move from individual to societal harms

This analysis of the privacy, freedom of expression and freedom of assembly harms of bulk interception shows how the real harms of bulk surveillance stems from the societal harms caused by their operation rather than any individual egregious act against a given individual. As argued by Richards the real harm to privacy posed by this form of large-scale surveillance should be thought of as the power imbalance given to the watcher and the chilling effect the knowledge of the bulk interception regime causes. This lines up well with the distinction that the privacy harm occurs when the data is accessed rather than collected but that the collection of this amount of data constitutes a societal harm in itself. This chilling effect can be most felt in the harms to freedom of expression and freedom of assembly, the knowledge of the ability of the state to monitor your communications in a political climate where the right to effective protest is being curtailed and there is an increasing emphasis on regulating online speech is going to have a large impact on a given individual's desire to exercise their rights. These

[75] Ilia Siatitsa, 'Freedom of assembly under attack: General and indiscriminate surveillance and interference and internet communications' (2020) 102 International Review of the Red Cross 181.
[76] Ibid.
[77] Peter Ullrich and Gina Rosa Wollinger, 'A surveillance studies perspective on protest policing: the case of video surveillance of demonstrations in Germany' (2011) 3 Interface: a journal for and about social movements 12.
[78] Valerie Aston, 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) 8 European Journal of Law and Technology 1.

harms in combination with the sheer scope of bulk interception presents an issue for the level of human rights protection which can be provided by European human rights law and the safeguards in place within the IPA which will be discussed further in the following chapters. While the approaches of the ECHR and CJEU may limit the possibility of abuse of these bulk surveillance powers, they are unable to protect against the harms caused by the normal, non-abusive, use of said powers.

5. Understanding Bulk Powers as Qualitatively Different from each other

While it is clear that bulk interception as operated under the Investigatory Powers Act regime is a broad, invasive intrusion into the protected rights of privacy, freedom of expression and freedom of assembly, it is not the only bulk power contained within this regime. The powers of bulk acquisition, bulk equipment interference and bulk personal datasets are also contained within this regime. This chapter aims to set out the capabilities of these powers and compare them with bulk interception. The human rights implications of bulk acquisition, equipment interference and personal datasets have received much less attention from human rights bodies than bulk interception with interception almost appearing to be a substitute for bulk surveillance.

5.1 Bulk Acquisition

Until publication of the draft bill for the Investigatory Powers Act in 2015, the existence of this capability was a tightly controlled secret. Section 94 of the bill empowers the Secretary of State to give providers of public telecommunications networks: "… such directions of a general character to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom".[1]

This capability is placed on a more precise statutory basis under sections 158 - 175 of the Investigatory Powers Act 2016. It gives the Secretary of State, on application of the Head of an Agency and after approval by a judicial commissioner, the power to issue a bulk acquisition warrant. This warrant cannot apply to the content of communications but may require a telecommunications operator to retain communications data and to disclose it to a person specified in the warrant. In contrast to Bulk Interception and Bulk Equipment Interference there is no requirement for bulk acquisition to be foreign-focused. The communications data of domestic communications such as phone calls and emails may be legitimately the intended focus for collection under the power.

The Code of Practice sets this out in finer detail in stating that a bulk acquisition warrant is:

> a warrant which authorises or requires the person to whom it is addressed to obtain the communications data described in the warrant from a telecommunications

[1] Investigatory Powers Act 2016 s 94.

operator, as well as authorising the selection for examination of the acquired communications data, as specified in the warrant.[2]

In Anderson's Review of the Bulk Powers Bulk Acquisition is described as providing "a broad spectrum of intelligence, with greater precision, speed, and often with less intrusion than other tools and techniques."[3] Only MI6 and GCHQ make use of the power[4] but claim that it used "on a daily basis". This claim was borne out at the time by the figures in the IOCCO report:

(a) "In 2015 GCHQ identified 141,251 communications addresses or identifiers of interest from communications data obtained in bulk pursuant to section 94 directions which directly contributed to an intelligence report."[5]
(b) "In 2015 the Security Service [MI5] made 20,043 applications to access communications data obtained pursuant to section 94 directions. These applications related to 122,579 items of communications data."[6]

The SIAs in question did not provide further detail on why such high numbers of applications were recorded. Approximately 5% of GCHQ's intelligence reporting each year contains material from at least one bulk acquisition source.[7] The majority of these reports are related to counter-terrorism, with other major areas including serious crime and certain geo-political reporting.[8]

Additionally, unlike the other powers discussed here, data obtained through bulk acquisition can be aggregated in one place. This distinguishes it from the data retention powers provided for successively by Regulations under the Data Retention Directive, by the DRIPA power, and now by Part 4 of the Investigative Powers Act. The existence of this aggregated database, as opposed to the federated databases kept by each Communications Service Provider (CSP) (subject to standard data retention obligations) is said to be a key element in the added value of the bulk acquisition power. The end product of Bulk Acquisition is then a massive aggregated database which provides SIAs with ease of access to the wealth of data the power

[2] Home Office, *Bulk Acquisition of Communications Data Code of Practice* (2018) para 1.2.
[3] David Anderson Q.C., *Report of the Bulk Powers Review* (2016) para 6.1.
[4] Ibid para 6.9.
[5] Ibid para 6.10.
[6] Ibid.
[7] Ibid para 6.11.
[8] Ibid.

collates. This end product highlights the broadness of the powers contained within the legislation.

Bulk Acquisition consists of a two-stage process: first, the obtaining of bulk collection data (BCD) from a CSP; and, second, the selection for examination of the BCD obtained under the warrant. This may also require a CSP to obtain and disclose specified communications data that is not in its possession but that it is capable of obtaining. A Bulk Acquisition Warrant normally provides for the provision of communications data as it is generated or processed by the CSP for business purposes but it may also provide for said data which is retained for business purposes or under the provisions of section 87 of the Investigatory Powers Act. This may likely result in the collection of large volumes of communications data, further showing the breadth of this power.

Notably, a Bulk Acquisition warrant need not be constrained to a specific operation. Additionally, as per section 158 there is no limit imposed on the volume of communications data which may be acquired. An example given in the draft code of practice is that if the requirements of the warrant are met then the acquisition of all communications data generated by a particular CSP could, in principle, be lawfully authorised but only where necessary and proportionate to do so.[9] This reflects the fact that bulk acquisition is considered an 'intelligence gathering capability' whereas targeted communications data acquisition is primarily an investigative tool that is used to acquire data in relation to specific investigations. Due to its nature as an 'intelligence gathering capability' a warrant for Bulk acquisition can only be sought by a member of the SIA. In addition, the volume of data which may potentially be acquired is reflected in the fact that bulk acquisition warrants must be granted by the Secretary of State and are subject to authorisation by the Judicial Commissioner. Once acquired in bulk, selection of data for examination is only permitted for approved operational purposes.

Although MI6 do not have Bulk Acquisition powers themselves, they cite the usefulness of bulk acquisition in their statement of utility. Stating that they depend on GCHQ's and MI5's use of bulk acquisition of communications data to develop an understanding of a threat to the UK, which MI6 can then use its assets and capabilities to inform and disrupt. This is cited as particularly important in the context of counter-terrorism and that said importance is unlikely

[9] Bulk Acquisition of Communications Data Draft Code of Practice para 3.5.

to decline.[10] GCHQ claims that in combination with the communications data obtained through bulk interception, this power is the primary way in which GCHQ discovers new threats to the UK. Without it, these threats would develop to fruition undetected until it was too late to stop them.[11]

At the time of writing, there have been no open descriptions of the product of Bulk Acquisition besides the usual explanations from the SIA: that GCHQ and MI5 state that they use them for the full range of their statutory functions, the categories of data requested will be subject to the bulk acquisition warrants discussed above and that categories of CSP may be in receipt of such directions or warrants. What has been openly described is that the IPA enables the SIAs to obtain large amounts of communications data, most of it relating to individuals who are unlikely to be of any intelligence interest.[12] Content cannot be obtained under the Act and bulk acquisition is not currently envisaged to obtain internet connection records. The primary thing that is known about the product is that it is collated in a massive single database rather than interspersed with the information collected through the other powers.[13] Here then the bulk acquisition power is emblematic of the powers contained with the IPA. It is a power which is broad in scope, capable of collecting immense amounts of data and operated covertly. Correspondingly strict safeguards are required in order to ensure this power's compatibility with the Convention.

Frustratingly, no programme revealed in the Snowden leaks meets the description of a bulk acquisition power as described by the IPA 2016. MUSCULAR and PRISM are two forms of acquisition but neither meet the UK legal definition of Bulk Acquisition. Outlining both will provide an insight into how bulk acquisition *may* be conducted by GCHQ. MUSCULAR is a joint initiative between GCHQ and the NSA to access the servers of Google and Yahoo in order to collect communications and communications data. This does not meet the description of BA outlined in the IPA as MUSCULAR involved the unauthorised access to the Google and Yahoo servers. PRISM is a program developed by the NSA which gave the Agency direct access to the servers of major internet providers such as Google, Apple, Skype, and Yahoo. GCHQ had access to PRISM since at least June 2010. PRISM is also arguably

[10] Ibid p 150.
[11] Ibid p 152.
[12] David Anderson QC, *Report of the Bulk Powers Review* (2016) para 2.40.
[13] Ibid.

not a form of Bulk Acquisition, but rather targeted acquisition as outlined by Cayford et al above.[14]

It is unclear whether PRISM is bulk or targeted acquisition. According to *The Guardian* article[15] which revealed it, the PRISM program gave the NSA direct access to the servers of major internet providers including Google, Apple, Skype and Yahoo. The article cites a 41 slide NSA PowerPoint presentation which speaks of "collection directly from the servers" of nine US ISPs.[16] The initial interpretation of this slide by *The Guardian* was that this meant said companies were collaborating with the NSA to give it a direct connection to their servers, to "unilaterally seize" all manner of communications from them; a form of bulk interception. GCHQ was alleged to have made use of the PRISM program as well.[17] However as per Cayford et al, this proved to be an error.

According to Cayford et al[18], the 'direct access' described above was access to a particular foreign account through a court order concerning that particular account. This was not wholesale access to all user's information from a given company. The court order gave the NSA access to the targeted account as well as to the accounts it was in contact with.[19] In this way PRISM followed the same principle of a court order on a phone number yielding the phone numbers the targeted phone has been in contact with. The NSA and the Attorney General serve a court order on the company in question for access to one or more foreign accounts. These accounts were then monitored and their activity is sent back to the NSA in real time as the NSA mirror the accounts. This was the 'direct access' described above. PRISM is then a targeted technology used to access court ordered foreign internet accounts[20] and thus does not fall under the category of Bulk Surveillance discussed in the rest of this chapter.

---

[14] Michelle Cayford, Coen Van Gulijk and Pieter Van Gelder, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014).
[15] Glenn Greenwald, Ewen MacAskill "NSA Prism program taps in to user data of Apple, Google and others" *The Guardian* (2013) https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
[16] Ibid.
[17] Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, Intelligence and Security Committee of Parliament.
[18] Michelle Cayford, Coen Van Gulijk and Pieter Van Gelder, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014).
[19] Ibid.
[20] Ibid.

However, Greenwald points out that this only applies when targeting a US citizen:

> "The NSA only need to obtain an individual warrant when it wants to specifically target a US person. No such special permission is required for the agency to obtain the communications data of any non-American on foreign soil, *even when that person is communicating with Americans.* Similarly, there is no check or limit on the NSA's bulk collection of metadata, thanks to the government's interpretation of the Patriot Act."[21]

This lines up well with the foreign focus safeguard contained with bulk surveillance legislation such as the Investigatory Powers Act wherein bulk powers must only be employed against individuals outside the nation state employing them. Interestingly, this safeguard is not applied to bulk acquisition under the Investigatory Powers Act. This point will be returned to in the later chapter on the UK legislative safeguards.

Following the reveal of PRISM Facebook and Google attempted to present PRISM as little more than a technical detail: a delivery system whereby the NSA receives data in a 'lockbox' that the companies are legally compelled to provide. Greenwald points out 4 issues which bely this argument. First, Yahoo fought PRISM vigorously in court which undermines the idea that PRISM was just a technical upgrade to an existing system. Second, *The Washington Post*'s Bart Gellman, upon receiving heavy criticism for 'overstating' the impact of PRISM, reinvestigated the program and confirmed his original claim that: "From their workstations anywhere in the world, government employees cleared for PRISM access may 'task' the system and receive results from an Internet company without further interaction with the company's staff."[22]

Third, while Facebook and Google denied that PRISM consisted of providing "direct access" or a "back door" respectively, these denials are more obfuscating than clarifying. The ACLU's tech expert has described these as highly technical terms of art denoting very specific means to get at information. The companies ultimately did not deny that they had worked with the NSA to set up a system through which the agency could directly access their customers' data.[23]

---

[21] Glenn Greenwald, *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. (Macmillan, 2014) p 112.
[22] ibid p 109.
[23] Ibid.

Fourth, the NSA itself has repeatedly hailed PRISM for its unique collection capabilities in multiple leaked slides. In one slide which makes the case using both PRISM and UPSTREAM, PRISM is described as having "Access to Stored Communications (Search)" and "Real-Time Collection (Surveillance)". In a slide titled 'PRISM Collection Details', a list titled 'What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In General:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File Transfers
- Video Conferencing
- Notifications of target activity – logins, etc
- Online Social Networking Details
- Special Requests[24]

On internal messaging boards, the Special Source Operation division frequently hails the massive collection value PRISM has provided. One message from November 2012 entitled "PRISM Expand Impact: FY12 Metrics":

> (TS//SI//NF) PRISM (US-984XN) expanded it impact on NSA's reporting mission in FY12 through increased tasking, collection and operational improvements. Here are some highlights of the FY12 PRISM program:
>
> PRISM is the most cited collection source in NSA 1st Party end-product reporting. More NSA product reports were based on PRISM than on any other single SIGAD for all of NSA's 1st Party reporting during FY12: cited in 15.1% of all reports (up from 14% in FY11). PRISM was cited in 13.4% of all 1st,2nd, and 3rd Party NSA reporting (up from 11.9% in FY11), and is also the top cited SIGAD overall.[25]

[24] Ibid p 110.
[25] Ibid p 111.

An internal NSA slide released by *the Guardian* clearly distinguishes between Upstream – Bulk Interception programmes including FAIRVIEW and BLARNEY – and PRISM which involves "collection directly from the servers of these US Service Providers: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube and Apple."[26] Types of data collected included a range of digital information such as email, chat, videos, photos, stored data, voice over internet protocol, video conferencing and online social networking details. An automated system called PRINATAURA organised the data by category. Some providers had the capability to provide real-time notification of an email event by target, such as a log-in.

5.1.1 Comparing Bulk Acquisition to Bulk Interception

Comparing bulk acquisition with bulk interception, we can see that there are a number of differences. While information about how bulk interception works is far clearer than bulk acquisition, they both nominally involve the collection of vast amounts of communications data. However, while interception involves the collection of traffic, application or network data as it crosses particular bearers, acquisition involves the collection of service-use metadata from communications servers. As discussed above, service-use metadata can be as identifying as application or content data. This would seem to disagree with the view of bulk acquisition from the SIAs in Anderson's report above that it is less intrusive and more precise than other powers. As mentioned above the sheer amount of communications data which GCHQ and MI6 have pulled from the use of this power belies their claim. While it is unclear whether PRISM is a clear example of how bulk acquisition works in practice, it is a good source of what such a program looks like. In terms of the expectation of privacy, given public knowledge of social media business practices – and the multitude of scandals over the use of personal data – it is reasonable to presume a lowered expectation of privacy when it comes to sharing data with a social media company. Bulk acquisition also bypasses peer-to-peer encryption through server-side collection in a way which interception does not.

5.2 Bulk Equipment Interference

[26] James Ball, 'NSA's Prism surveillance program: how it works and what it can do' *The Guardian* (2013) (https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google) accessed 09/06/2022

Bulk Equipment Interference covers a range of techniques involving interference with computers, the majority of which were previously known as computer network exploitation (CNE). While Equipment Interference (EI) includes more well-known techniques such as hacking or the implantation of software into endpoint devices or network infrastructure to retrieve intelligence, it can be as simple as copying data directly from a computer. EI is becoming increasingly useful to SIAs when compared with bulk interception practices. This is due to the fact that targets on which SIAs would use bulk interception have begun to use encryption as a means of bypassing this. EI renders any such peer to peer or end to end communication encryption moot by accessing the communications data at its origin, the device itself.

The draft IPA code of practice provides a description of what constitutes equipment interference: "Equipment interference warrants authorise all actions necessary for the obtaining of communications, equipment data or other information from equipment."[27] This interference can be carried out both remotely and by physically interacting with the equipment. The range of this interference is presented as a scale. At the lower end of the scale an agency conducting EI may covertly download data from a subject's mobile phone when left unattended. At the higher end said agency may exploit existing vulnerabilities in software in order to either gain control of devices or remotely extract data or to monitor the user of the device.[28] It is unclear what this is supposed to mean in practice for bulk equipment interference warrants, and it may be being left purposefully vague. It could mean the mass installation of malware or viruses onto smartphones, laptops and PCs. It could also mean collaboration with tech companies to install backdoors into their encryption for SIAs to exploit.

In February 2016, the Investigatory Powers Tribunal recorded a number of admissions by the Government on the use of EI, which was then referred to as CNE. These included that GCHQ carries out CNE within and outside the UK and that in 2013 about 20% of GCHQ's intelligence reports contained information derived from CNE. There are both "persistent" and "non-persistent" CNE operations. A persistent operation is where an implant resides on the computer in question for an extended period, versus a non-persistent operation which expires

[27] Home Office, *Equipment Interference Code of Practice* (2018) para 3.11.
[28] Home Office, *Equipment Interference Code of Practice* (2018) paras 2.1 – 2.4.

at the end of a user's internet session. CNE operations undertaken by GCHQ can be against a specific device or a computer network.[29]

It was further acknowledged that CNE/EI *might* be used by GCHQ so as to involve the following:

i. the obtaining of information from a particular device, server or network;
ii. the creation, modification or deletion of information on a device, server or network;
iii. the carrying out of intrusive surveillance;
iv. the use of CNE in such a way that it creates a particular security vulnerability in software or hardware, in a device or on a network;
v. the use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest (referred to as bulk CNE);
vi. the use of CNE to weaken software or hardware at its source, prior to its deployment to users; and
vii. the obtaining of information for the purpose of maintaining or further developing the SIAs' CNE capabilities.[30]

The dividing line between large scale targeted and/or thematic EI and Bulk EI is not clear. A Bulk EI Warrant may authorise interference with any equipment for the purpose of obtaining (a) communications, (b) equipment data, and (c) "any other information". It should be noted again that bulk warrants can only do so provided that there is a foreign focus. As of 2016 GCHQ had not conducted any operations which could be authorised by a bulk EI warrant.[31] However given the increasing problem encryption presents to SIAs it is likely that bulk EI will become more commonly used in the future. A leaked letter written in 2018 by then Minister of State for Security and Economic Crime , Ben Wallace, outlines how: "following a review of current operational and technical realities, GCHQ have revisited the previous position and determined that it will be necessary to conduct a higher proportion of ongoing overseas focused operational activity using the bulk EI regime than was originally

[29] Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ [2016] UKIPTrib 14_85-CH, para 5.
[30] Ibid para 9.
[31] Report of the Bulk Powers Review 2016 p 123.

envisaged."[32] This information is a result of a leak and so must be treated with caution, but considering the SIAs face the observable technical reality of apps such as WhatsApp and Signal, it is probable that GCHQ will re-evaluate their position on bulk EI.

Bulk equipment interference warrants are issued under chapter 3 of part 6 of the IPA 2016.[33] They may only be issued to intelligence services and the main purpose of a BEI warrant must be limited to the acquisition of overseas-related communication, equipment data and/or information.[34] It authorises or requires:

> The person to whom it is addressed to secure interference with equipment for the purpose of obtaining the communications, equipment data or other information described in the warrant and/or to select for examination such material. A BEI warrant must set out specific operational purposes (see also paragraph 6.66). No material may be selected for examination unless doing so is necessary for one or more of the operational purposes specified on the warrant.[35]

At the time of Anderson's review of bulk powers Bulk Equipment interference was unique in that it had not yet been used.[36] As of 2021 this is not the case; 3 BEI warrants were approved in 2018 and 10 in 2019.[37] The main operational case for both targeted and bulk equipment interference is tied to diminishing returns from interception owing to technical developments such as end-to-end encryption and the increasing anonymisation of network devices which makes it harder to distinguish between target and non-target devices without at least some initial analysis of the data held on them:

> Terrorist, serious criminal and hostile states have embraced technological advancements, including the widespread use of encryption, and the growth of the internet to hid from sight and to plan their attacks. As a result of this, the security and intelligence agencies can no longer rely solely on interception and are faced with an increasingly partial and fragmented intelligence picture, even when investigating known threats. If the security and intelligence agencies are to be able to maintain the

[32] Tech Dirt, 'UK Spies Say They're Dropping Bulk Data Collection For Bulk Equipment Interference' <https://www.techdirt.com/2018/12/12/uk-spies-say-theyre-dropping-bulk-data-collection-bulk-equipment-interference/> accessed 25/03/2022.
[33] Investigatory Powers Act 2016 s 176 – 198.
[34] Ibid s 176 (1)(c).
[35] Equipment Interference Code of Practice (2018) para 6.2.
[36] David Anderson Q.C., *Report of the Bulk Powers Review* (2016) para 7.1.
[37] IPCO, *Annual Report*, 2018; IPCO, *Annual Report of the Investigatory Powers Commissioner*, 2019.

> same understanding of threats and be able to disrupt them, they need to use other, and complementary, techniques which will provide comparable pieces of the intelligence jigsaw[38]

The draft EI code of practice provides a useful example of a bulk equipment interference warrant in practice. In the example intelligence suggests that a terrorist cell in a particular location in the Middle East is plotting an imminent bomb attack against UK interests in the region. While little is known about the individual members of the cell, it is known that a particular software package is commonly used by some terrorist groups. Unfortunately, the level of specificity in the example is limited to "using equipment interference to obtain equipment data from a large number of devices in the specified location." Fortunately, it goes into further detail on the filtering and selection for examination processes: "officers apply analytical techniques to the data, starting with a search term ('selector') related to the known software package, to find common factors that indicate a terrorist connection." A series of refined searches are conducted, using evolving factors that are uncovered during the course of the analytical process. This process gradually identifies devices within the original 'pot' of data collected that belong to the terrorist cell. Their communications (including content) can then be retrieved and examined.[39] While this example provides a clear picture of the process of filtering and selecting data for examination, it leaves a large gap in terms of how this data is collected in practice. Hence it is necessary to fill out this picture using the Snowden leaks.

Unlike bulk acquisition there are a number of programmes revealed by the Snowden leaks which can reasonably be described as equipment interference, it as also known as computer network exploitation (CNE) or Active SIGINT. Each involves implanting malware directly onto a user's computer. These programmes can be reasonably divided into three methods: hardware, software, and secret servers.

Examples of equipment interference through the use of software in the Snowden files include NOSEY SMURF which involved implanting malware to activate the microphone on smart phones, DREAMY SMURF, which had the capability to switch on smart phones, and TRACKER SMURF which had the capability to provide the location of a target's smart phone with high-precision, and PARANOID SMURF which ensured that the malware remained hidden. DROPOUTJEEP is an Apple iphone software hack, and SOMBERKNAVE

[38] David Anderson Q.C., *Report of the Bulk Powers Review* (2016) para 7.2.
[39] Equipment Interference Code of Practice (2018) para 6.5.

– a Windows XP attack - which uses the computer's unused wireless device as a means of access and control of the device. OPTIC NERVE gained particular notoriety as it captured the entirety of the Yahoo webcam's footage for a given amount of time. Similarly, to this GUMFISH can covertly take over a computer's webcam and snap photographs. GROK is used to log keystrokes, and FOGGYBOTTOM records logs of internet browsing histories and collects login details and passwords used to access websites and email accounts.

Examples of hardware interference include: IRATEMONK, which is firmware installed onto hard drives, below the operating system in the physical workings of the disk. This is claimed to work on Western Digital, Seagate, Maxtor, and Samsung disks tracks what the computer is doing. This will stay even if the disk is wiped out, repartitioned and/or reformatted. HOWLERMONKEY is a ethernet port bug. COTTONMOUTH is a wireless transmitter in a USB cable. RAGEMASTER is a wireless transmitter in a VGA cable. SALVAGERABBIT exfiltrates data from removable flash drives that connect to an infected computer.

QUANTUMINSERT involved the use of fake duplicate websites, or secret servers, to gain access to computer networks, this was used as part of a GCHQ project called OPERATION SOCIALIST in order to gain access to Belgacom's servers. This was also employed against users of the Tor (The Onion Router) browser, a programme employed by its users to ensure anonymity. Once a tor user is identified QUANTUM servers are employed to redirect the user towards other secret servers called FOXACID. Because QUANTUM servers are stationed at key locations on the internet backbone they can react faster than the other websites and thus impersonate the website the user is trying to access,[40] this is known as man-in-the-middle positioning.[41] Once the computer in question has been redirected to a FOXACID server the server determines the best way by which to attack the computer in question. In the case of Tor it attacks through the Tor browser bundle and vulnerabilities in the associated Firefox browser. Once an attack has been successful, the infected computer will call back to the FOXACID server, which then further infects the computer, compromising it long-term.[42] GCHQ was also said to have gained access to via CNE to the

[40] Michelle Cayford, Coen Van Gulijk and Pieter Van Gelder, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014).
[41] Ryan Gallagher and Glenn Greenwald. "How the NSA plans to infect 'millions' of computers with malware" March 12, 2014 *https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.*
[42] Ibid.

entire network of a company called Gemalto, which produces SIM cards, including their encryption case.

TURBINE provides the clearest picture of a bulk equipment interference programme in that it allows "the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually."[43] It was designed in response to the problem of scale: "Human 'drivers' limit ability for large-scale exploitation (humans tend to operate within their own environment, not taking into account the bigger picture)".[44] TURBINE was described in the Snowden files as an "intelligent command and control capability" that enables "industrial scale exploitation." The system has been operational since at least July 2010 and early reports on the Snowden files indicated that the NSA had already deployed between 85,000 and 100,000 implants against computers and networks worldwide, with plans to increase those numbers.[45]

Another example of the NSA's use of bulk equipment interference is SECONDDATE. According to a leaked presentation slide is described as allowing "mass exploitation potential for clients passing through network choke points, but is configurable to provide surgical target selection."[46] This is done through the use of man-in-the-middle positioning and its similarities to bulk interception bare mentioning. They both use specific bearers in the fibre optic cables which make up the backbone of the internet but whereas bulk interception programs such as TEMPORA or UPSTREAM collect communications data, SECONDDATE uses these bearers to implant malware onto devices it deems to be of intelligence value.

SECONDDATE and TURBINE both rely on the TURMOIL network of sensors which has bases in Misawa, Japan and Menwith Hill, England. The sensor network operates as a dragnet, monitoring packets of data as they are sent across the Internet. According to another leaked slide the NSA operates the base in Menwith Hill in close cooperation with GCHQ. The same slides reveal that the Menwith base has been used to experiment with implant exploitation attacks against users of Yahoo and Hotmail.[47]

---

[43] Electronic Frontier Foundation, '20140315-Intercept-TURBINE Intelligence Command and Control' (2014) <https://www.eff.org/document/20140315-intercept-turbine-intelligence-command-and-control> accessed 03/03/22.
[44] Ryan Gallagher and Glenn Greenwald. "How the NSA plans to infect 'millions' of computers with malware" March 12, 2014 *https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.*
[45] Ibid.
[46] *Ibid.*
[47] Ibid.

There are points here which require some clarification. As has been referenced in the Bulk Acquisition section, it is difficult to prove whether specific NSA and GCHQ programs revealed in the Snowden files were targeted or bulk in their operation. It is important to note however, the amount of different applications of equipment interference - targeted and bulk - available to SIAs and how they vary from the application of bulk interception and bulk acquisition. From an expectation of privacy standpoint, there is an argument that the act of sending a communication online or sharing your data with a social media platform carries with it the knowledge of potential interception or acquisition. However, the same cannot be said for simply using a computer or phone to store files, accessing a website, using a specific browser which is designed to ensure privacy. It is difficult to reconcile the claim of the SIAs that as of the writing of Anderson's review they had not used the bulk equipment interference power. Nonetheless, they have in subsequent years used it although to a much lesser extent than bulk interception or acquisition.

5.2.1 Comparing Bulk Equipment to Bulk Acquisition and Bulk Interception

Continuing this comparison to interception and acquisition: bulk equipment interference would seem to comprise a number of different methods. Implantation of malware electronically through viruses, implantation of malware through secret servers and the physical implantation of hardware. The secret server methods – SECONDDATE and TURMOIL – would seem to rely on the same bearers as bulk interception. This is useful as a comparative example of intrusiveness. If we take the use of such bearers to intercept communications data as a baseline of intrusiveness, how much more intrusive is using these bearers to directly interfere with an individual's electronic device? Considering that such interference provides access to sensitive and identifying data which the individual never intended to share, the corresponding expectation of privacy must be far higher. Similar to bulk acquisition, equipment interference bypasses peer-to-peer encryption which bulk interception struggles to do which may point to its increased use in upcoming years.

5.3 Bulk Personal Datasets

The fourth and final bulk power is the ability to retain and use Bulk Personal Datasets (BPD). While SIAs recognised the value of BPDs as far back as the beginning of the century, the power was first formally disclosed in the 2015 ISC Report. As per the operational case for BPDs put forward by the SIAs:

> Bulk personal datasets comprise personal data relating to a number of individuals, the majority of whom are unlikely to be of intelligence interest. The security and intelligence agencies hold the data electronically and analysts will only look at the data relating to the minority who are of intelligence interest. The security and intelligence agencies do this by asking specific questions of the data to retrieve information of intelligence value.[48]

Specific examples of BPDs disclosed include the passport register, the electoral register, the telephone directory and data about individuals with access to firearms. Broader categories disclosed include law enforcement/intelligence, travel, communications, finance, population, and commercial. BPDs generally contain basic biographical details on individuals that will correspond to the definition of "identifying data". Those who have seen the full list of datasets include Dominic Grieve QC MP, former Chair of the ISC, who described them as "pretty mundane".[49]

The IPA doesn't provide the power to acquire or obtain new BPDs as this power already exists under the Security Service Act 1989 and Intelligence Services Act 1994 (known as the information gateway provisions).[50] Under these Acts, BPDs can be acquired through both overt and covert means. According to the case studies provided in the Report, they are used on a daily basis in combination with other capabilities, across the range of the SIAs' operations.[51]

Two types of warrant are provided for in the IPA. Class BPD warrants which authorise the retention and use of a particular class of BPD, and specific BPD warrants. However, both warrants governing the use of BPDs are considered bulk warrants due to how even the request of a single BPD is likely to contain data on persons not currently targets. BPDs are still largely held by individual SIAs although copies may be shared with other SIAs via the legal gateway provisions in SSA 1989 and ISA1994, and individual officers may access data held by a different SIA on an ad hoc basis when authorised to do so. MI6 and MI5 currently have a greater reliance on BPDs than GCHQ. There is a cross-SIA mandate to work more collaboratively across the SIAs in sharing BPDs. The searching of BPDs is performed in a way that is analogous to commercial techniques. Whilst SIAs claim that their methods are

[48] David Anderson QC, *Report of the Bulk Powers Review* (2016) p 41.
[49] Ibid.
[50] Ibid .
[51] Ibid p 192.

behind commercial techniques, they see themselves as "catching up with the commercial sector".[52] Any critical view of the BPD power must assume that this is the case and that they will inevitably catch up with the commercial sector. The IPA has provided SIAs a series of updated powers which are capable of keeping pace with modern communication technology. However, these powers are broad in reach and scope and require tightly defined definitions of who and what they may be applied to.

Bulk Personal Datasets (BPDs) are described as "a set of data that has been by an intelligence service comprises a BPD where it includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the intelligence services in the exercise of their statutory functions."[53] These datasets are typically "very large, and of a size which means they cannot be processed manually."[54]

All three SIAs retain and use BPDs, though GCHQ uses them to a lesser extent than MI6 and MI5.[55] The operational case describes BPDs as "an essential tool" for the SIAs, without which "the security and intelligence agencies would be significantly less effective in protecting the UK against threats such as terrorism, cyber threat or espionage."[56]

> BPD enables the security and intelligence agencies to focus their efforts on individuals who threaten national security or may be of other intelligence interest, by helping to identify such individuals without using more intrusive investigative techniques. It helps to establish links between subjects of interest or better understand a subject of interest's behaviour. BPD also assists with the verification of information obtained through other sources (for example agents) during the course of an investigations or intelligence operation... Using BPD also enables the security and intelligence agencies to use their resources more proportionately because it helps them exclude potential suspects from more intrusive investigations.[57]

MI5 has stated that it uses BPD to "quickly develop fragmentary intelligence into a real world identity".[58] Similarly, for MI6, BPD "often form the backbone of investigative work"

[52] Ibid p 44.
[53] Bulk Personal Datasets Code of Practice para 2.2.
[54] Ibid.
[55] David Anderson Q.C., *Report of the Bulk Powers Review* (2016) para 8.1.
[56] Ibid.
[57] Ibid para 8.2.
[58] Ibid para 8.3.

which enables MI6 to "take a piece of fragmentary information and make a positive identification of a person of intelligence interest who could not otherwise be identified".[59] BPDs are described as being important across all of MI6's operational areas such as counter-terrorism, counter-proliferation, cyber, serious crime and the geographical requirements. GCHQ added that BPDs are used primarily to "enrich" information that it had obtained through other means.[60]

In terms of Snowden file comparisons, BPDs are difficult to find an exact match. The easiest comparison is made with the various databases employed by the NSA. The Intercept reported on a flat data store codenamed BLACK HOLE based on a leaked GCHQ powerpoint presentation slide. At the time of the slides creation in 2009 the store weighed in at 217 terabytes when uncompressed, and consisted entirely of metadata; notably 41% HTTP data or browser histories, 19% web search data and 12% SMTP data.[61] Over the course of two years, 2007 to 2009, Black Hole was used to store more than 1.1 trillion events, with about 10 billion events per day. Events is the term used by GCHQ to refer to the lodging of metadata records. By 2010 GCHQ was logging 30 billion events a day and at the time of the Snowden leaks in 2012 collection had reached 50 billion events per day.[62] If BLACK HOLE was a exact example of a BPD, this would be a damning comparison but they don't quite line up. BLACK HOLE appears to be where all the data collected by the powers discussed in the previous sections is stored. Whereas a BPD seems to draw its data from registries and other databases where individuals have identified themselves such as passport registries, airline ticket databases, oyster card sign-ups. These examples are all related to travel as the government has given travel data as one of its few specific examples of a BPD. So then, while BPD data is not collected in an intrusive manner, it does contain highly identifiable data.

The Government claims that BPDs are used by the SIAs "on a daily basis, in combination with other capabilities, right across the security and intelligence agencies' operations."[63] All investigative staff and analysts at MI5 have access to BPDs, although some of the datasets are

[59] Ibid para 8.4.
[60] Ibid.
[61] Alexander J Martin "Blighty's GCHQ stashes away 50+ billion records a day on people." The Register September 25, 2015 https://www.theregister.co.uk/2015/09/25/trillions_in_surveillance_gchq/.
[62] Ryan Gallagher "Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities" The Intercept September 25, 2015 https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.
[63] David Anderson Q.C., *Report of the Bulk Powers Review* (2016) para 8.7.

restricted to analysts only. This drops to 80% of people working on intelligence operations in MI6 having access to BPDs. This drops even further to only 10% of those working on intelligence operations at GCHQ having access to BPDs.[64] In general GCHQ uses bulk personal dataset in conjunction with other powers to identify new targets and to enrich our knowledge of existent targets. Examples are given of confirming a target's identity and discovering new connections and networks. GCHQ divides its activities into three stages Identify, Understand, and Action. It is in the Identify stage where GCHQ sees the importance and use of BPD as increasing. With the latter stages GCHQ sees BPD's importance remain the same for GCHQ. This points to BPD as a supportive power for use with the other powers.

Given the information which is, likely, present in these datasets, it is unlikely that the BPDs could be used to find threats by itself. GCHQ frames the use of the bulk powers in general into two categories. Bulk interception and bulk equipment interference are framed as primary means by which to intercept threats, while bulk acquisition and bulk personal datasets are framed as means of minimising "intrusion into privacy when seeking to identify new leads and can also be used to provide GCHQ with the assurance that an account targeted for more intrusive content collection does not belong to a UK individual."[65] While this seems likely true for BPDs, as discussed above it is unlikely to apply to Bulk Acquisition in practice. There is also the question of the identifying nature of this data. While it may not be collected in an intrusive manner, this data is by definition and function identifying. This creates a tension with the UK implementation of the GDPR as discussed above in the section on metadata. Nonetheless, it is clear that the retention and use of bulk personal datasets is qualitatively different to the other bulk powers described here.

5.4 Comparing and Categorising Bulk Powers

In 2016, GCHQ usefully provided a statement of utility of bulk capabilities where they explained how the powers are increasing or decreasing in importance. These evaluations are divided into three stages: Identify, Understand, and Action. The 'Identify' stage is described as where GCHQ interrogates collected communications data to answer questions about developing incidents as they occur and identify the individuals involved. Here the importance of bulk interception is described as either remaining the same or as being in decline. Bulk

[64] Ibid para 8.8.
[65] David Anderson Q.C., *Report of the Bulk Powers Review* (2016) p153.

acquisition is described as remaining the same. However, the importance of bulk equipment interference and bulk personal datasets are described as increasing in importance.[66]

The 'Understand' stage describes the ability of GCHQ to understand the plans and actions of individual terrorists, criminals, and other targets in order to disrupt or frustrate their plans. Here bulk interception is described as remaining the same level of importance for cyber defence while declining for non-cyber defence. BPDs are described as remaining the same for GCHQ, and bulk acquisition is described as remaining the same or being in decline. Again, equipment interference is described as increasing in importance.[67] The 'action' stage describes the utility of the analysis produced from examining the data collected by the various bulk powers. Each power as the same evaluation of importance as in the 'understand' stage.[68]

Across each of these stages, bulk interception and acquisition appears to either be stagnant or declining in use. At the identify stage bulk personal datasets are seen as increasing in importance but remaining the same in the other stages. Only bulk equipment interference is seen as increasing in importance across all three stages. This is a key way in which to compare and categorise the bulk powers as the increasing use of the most intrusive bulk power warrants discussion as to the human rights implications of such use as well as the safeguards surrounding that power.

5.5 Conclusion

From the outlines of the various powers above, it is possible to compare and categorise the bulk powers available under the IPA. There are multiple ways in which to do this. As previously mentioned, the official narrative is to split them into threat-finding powers – BI and BEI – and complementary powers – BA and BPD. However, this does not line up with how they operate in practice. If a power is meant to be threat finding via the quantity of communications data it intercepts then bulk acquisition is a threat-finding power. Another way to split them is in terms of their ability to bypass encryption with BI and BPD being largely unable to do so and BA and BEI being able to bypass encryption entirely by collecting the data prior to encryption. A further way to categorise them is in terms of expectation of privacy. This category is less concrete as you can argue each way as to the

[66] David Anderson Q.C. 'Report of the Bulk Powers Review' (2016) p152.
[67] Ibid.
[68] Ibid.

expectation of privacy a person may have when sending a communication, sharing data with a social media company or giving their details to the passport registry. BEI is an exception to this as it is difficult to see a way in which a person expects their private electronic device to be implanted with malware. The main takeaway here is that each of the bulk powers contained within the IPA is qualitatively different from the others in terms of use, impact and design. There is also a question of the different types of data which each power collects and retains, how much more or less identifying is equipment data when compared to traffic data? How does bypassing encryption affect the expectation of privacy of the user? As will be discussed in the chapter on the Investigatory Powers Act, the current safeguards for the use of these powers do not adequately reflect the differences between them.

This presents a problem from a human right perspective. As will be discussed in upcoming chapters the primary test for the compatibility of bulk surveillance with the ECHR is the presence of adequate and sufficient safeguards against abuse. Though the Court has ruled that the safeguards for bulk interception under RIPA are adequate and effective, it should not be assumed that these safeguards are sufficient for bulk equipment interference, acquisition, or bulk personal datasets. The latter three were not covered under RIPA having been introduced in the IPA 2016. Stretching the bulk interception safeguards to cover the other powers obfuscates the different human rights implications of these powers and provides opportunities for the executive to abuse these powers. Given that the SIAs claim that their use of encryption bypassing powers such as bulk acquisition and equipment interference will increase in coming years, this is a gap which should be filled. This thesis will construct safeguards which are tailored to these powers in line with ECHR jurisprudence.

6. Bulk Interception Caselaw of the ECHR

The following chapter continues to cover the development of the ECHR case law on surveillance, namely the Court's approach to bulk surveillance. The end product of this development provides the means by which to assess the convention compatibility of the surveillance regime under the Investigatory Powers Act 2016. The key aspect of the ECtHR's approach to bulk surveillance is the *Weber* requirements. As of the 2021 *Big Brother Watch* GC judgment they are a series of minimum requirements which must be incorporated into bulk surveillance regimes which include:

1. The grounds on which bulk interception may be authorised;
2. The circumstances in which an individual's communications may be intercepted;
3. The procedure to be followed for granting authorisation;
4. The procedures to be followed for selecting, examining and using the intercept material;
5. The precautions to be taken when communicating the material to other parties;
6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. The procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[1]

This chapter charts the development of the ECtHR's approach to bulk surveillance through the development of the *Weber* requirements. The trend of technological development examined in the previous chapter is prominent here. The timeline of this chapter ranges from 2006 until 2021 and can be extended further if one considers that the first case *Weber* was lodged domestically in the late 1990s. Where *Weber* concerns telephones, emails and faxes, 12 years later *Big Brother Watch* concerns the interception of all electronic communications as they cross transatlantic cables. This is an exponential rate technological development across a relatively short period of time which the Court has attempted to account for. Simultaneously the second trend observed in the previous chapter, the covert nature of surveillance, remains the same. As these surveillance operations become larger, wider in

[1] *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 361.

scope and able to collect exponentially greater amounts of data, the Court has access to the same level of publicly available information as it does with targeted surveillance cases. In some cases the Court has less information as it is increasingly difficult to prove victim status and adduce evidence of actual surveillance. While it may have been possible to prove that you were being physically subjected to surveillance in the past, modern bulk surveillance makes it near impossible to prove that one has been subjected to surveillance. These twin threads are observed throughout these cases. These trends are particularly noticeable as the Court attempts to use a set of safeguards designed to assess targeted surveillance regimes on bulk surveillance regimes.

The chapter divides this development into 5 stages, beginning with the establishment of the *Weber* safeguards in 2006 and ending with the establishment of 'end-to-end safeguards' in 2021. Stage two covers two cases against the UK surveillance regime under RIPA: *Liberty* (2009) and *Kennedy* (2011), where the Court first established an *in abstracto* approach to bulk surveillance. A significant development which enabled the Court to consider the Convention compatibility of increasingly covert bulk surveillance regimes without requiring an individual applicant to prove victim status. Stage three covers two cases wherein the respective surveillance regimes allowed too much discretion to the executive: *Zakharov* (2016) and *Szabo & Vissy* (2016). In this stage, the Court refined both the requirements for victim status and clarified exactly how an *in abstracto* review of surveillance legislation would be conducted. Stage four covers the first chamber judgments of the first two post-Snowden revelations bulk surveillance cases: *Centrum fur Rattvisa* (2018) and *Big Brother Watch* (2018). In this stage the Court attempts to alter the *Weber* requirements to better fit modern bulk surveillance regimes, while simultaneously accepting the operation of said regimes as being within a state's margin of appreciation. Finally, stage five covers the Grand Chamber judgments of *Centrum* and *Big Brother Watch* (2021), wherein the Court transforms the *Weber* safeguards into a new set of 'end-to-end' safeguards. Despite this transformation the new safeguards bare multiple similarities with the old safeguards, and will require further evolutive change in order to effectively safeguard the realities of contemporary bulk surveillance. This chapter uses these five stages to demonstrate the evolutive change in the Court's approach over 15 years of jurisprudence, and to highlight where this evolution should continue.

6.1 Bulk Surveillance Case Law: A Typology

It is useful first to define some key terms which will be used throughout this chapter. As discussed in chapter one, the term 'Mass surveillance' is imprecise in that it covers a multitude of surveillance apparatuses. It also carries multiple meanings and multiple subcategories. Bulk surveillance by contrast is more precise and has a basis in the ECtHR's jurisprudence. There is some inconsistency to clarify here as the Court has only recently began using the term bulk surveillance to describe these surveillance apparatuses:

Case	**Bulk or targeted surveillance case**	**Surveillance Apparatus description**
Weber and Saravia	Bulk	Strategic Monitoring
Liberty v UK	Bulk	Interception of External Communications
Kennedy v UK	Targeted	Interception of Internal Communications
Zakharov v Russia	Targeted	Interception of Mobile Phone Communications
Szabo and Vissy v Hungary	Targeted	Interception of Communications
Centrum fur Rattvisa v Sweden	Bulk	Bulk Signals Intelligence/Bulk Interception of Communications
Big Brother Watch v UK	Bulk	Bulk Interception of Communications

Table 1: ECtHR Classification of Bulk Surveillance Regimes

The Court only began referring to surveillance apparatuses as bulk in the first chamber judgment of *Centrum fur Rattvisa*. Here, the Court acknowledged that it had considered the Convention compatibility of bulk interception regimes on two previous occasions: *Weber*, and *Liberty*.[2]

[2] *Centrum för Rättvisa v Sweden* (2018) 68 EHRR 2 para 108.

The above table also points towards other terms in need of clarification, such as the distinction between internal and external interception of communications. The distinction between external and internal surveillance regimes lies in both the origin of the communication and the end-point of a communication. For example, An external communication is one which either originates outside of the UK or originates inside the UK and is sent to a recipient outside of the UK. For a communication to be considered internal it must begin and end within the UK.

Finally, in the jurisprudence of the Court, the only form of bulk surveillance which has been considered is bulk interception. This does not mean that the terms bulk surveillance and bulk interception are synonymous in the eyes of the Court, but rather that an application considering bulk acquisition or bulk equipment interference has not been considered by the Court as of the writing of this thesis. What can be considered synonyms of bulk interception are the terms in the table above for *Weber, Liberty*, and *Centrum.* Each refers to a surveillance apparatus which allows for untargeted, large-scale, interception of external communications.

6.2 Stage 1 (2006): Establishing the *Weber* Requirements

Weber and Saravia v. Germany is considered the first time the Court looked at bulk surveillance. This is the beginning of the Court's distinction between mass or blanket surveillance and bulk surveillance. While the former is prohibited the Court is willing to allow the latter provided adequate safeguards are present. *Weber* concerned the same (amended) legislation as *Klass v. Germany*, the first time the Court addressed the secret surveillance of communications. In *Klass* the legislation at issue laid down a series of limitative conditions which had to be satisfied before a surveillance measure could be imposed. The permissible restrictive measures were then confined to cases in which there were factual indications for suspecting a person of planning, committing, or having committed certain serious criminal acts. These measures could only be ordered if gaining this information was impossible or much more difficult without surveillance and said surveillance could only cover the specific suspects or those he was in contact with. Importantly the Court observed that "so-called exploratory or general surveillance was not permitted by the contested legislation,"[3] which allowed the Court to take a less stringent approach to the

[3] *Klass and Others v. Germany* (1979) Series A no.28 para 51.

necessity of the measures.[4] The Court distinguished between individual and strategic monitoring by pointing out that individual monitoring "serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed."[5] The key to this is individualised suspicion.[6] By contrast the strategic monitoring examined in *Weber* was "aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany."[7] While the strategic surveillance regime did not constitute blanket surveillance of the entire population, its collection was indiscriminate to whether there was any suspicion of criminal involvement.[8]

This admissibility decision concerns the interception of two applicant's communications. Nevertheless, it is an important and influential judgment, having been cited multiple times in bulk surveillance case law. Weber was a German freelance journalist who investigated areas which are generally subject to surveillance by the German authorities such as gun running or drug smuggling.[9] In her work she travelled often throughout Europe and South America. Saravia was an employee of Montevideo City Council, Uruguay, who took messages for Weber on their phone.[10] Both applicants were in Uruguay when the interception happened in the early 1990s with the initial complaint to the German Constitutional Court occurring in 1995.[11] The date of the Court's final judgment is ten years later in 2006. The case concerned The Act of August 13, 1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications, also called the G10 Act. The act was amended in 1994 which extended the range of subjects who could be subject to 'strategic monitoring' (as opposed to monitoring of individuals). They alleged that certain provisions of the amended G10 Act infringed their rights under the German Constitution and in turn their rights under Article 8 ECHR.

[4] *Big Brother Watch,* Partly Concurring, Partly Dissenting Opinion of Judge Koskelo, joined by Judge Turkovic. P 25.
[5] *Weber and Saravia v Germany* (2008) 46 EHRR SE5 4.
[6] Maria Helen Murphy. "Algorithmic Surveillance: the collection conundrum." (2017) 31 International Review of Law Computers & Technology 225-242, 234.
[7] *Weber and Saravia v Germany* (2008) 46 EHRR SE5 4.
[8] Maria Helen Murphy "Algorithmic Surveillance: the collection conundrum." *International Review of Law Computers & Technology,* 31m no. 2 (2017): 225-242, 234.
[9] *Weber and Saravia v Germany* (2008) 46 EHRR SE5 para 5.
[10] Ibid para 6.
[11] Ibid para 7.

It is important contextually to note that the surveillance (strategic monitoring) in question was carried out on telephone, telex and fax communications with an expansion to email planned in future. As the Court has gone on to use the test set out in *Weber* more and more, an evolutive interpretation of these tests would be desirable in order to better fit more contemporary forms of bulk surveillance. *Weber* can thus be seen as a crossroads for the Court. From here the Court could have taken its bulk surveillance jurisprudence in two directions. The first would be an evolutive increasingly strict path which accounts for the evolving and rapidly expanding nature of surveillance technology. The other path would be a more deferential path with increasingly recommended but not required safeguards. As will be demonstrated over the following stages, the Court chose the latter.

6.2.1 The Weber Requirements

In its deliberations in *Weber* the Court focused on the 'in accordance with the law' test and determined a set of criteria for determining the lawfulness of secret surveillance and interception of communications and to avoid 'abuse of powers' and arbitrariness:

> It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated … The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures…[12]

Additionally, the Court stated that "it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power." As a result of this "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".[13] It is important to note that the Court was here citing *Huvig v France*, a case concerning targeted surveillance via telephone tapping as a key source in this first mass surveillance case. This is important as the Court then set out its test of minimum requirements that must be provided for in the domestic legislation

[12] *Weber and Saravia v. Germany* App no. 54934/00 (ECHR, 29 June 2006) para 93.
[13] Ibid, para 94.

for testing whether the said law was sufficiently foreseeable.[14] Specifically, the criteria established were:

1. the nature of offences which may give rise to an interception order;

2. a definition of the categories of people liable to have their communications intercepted;

3. a limit on the duration of interception;

4. the procedure to be followed for examining, using and storing the data obtained;

5. the precautions to be taken when communicating the data to other parties; and,

6. the circumstances in which intercepted data may or must be erased and destroyed.[15]

These are the same requirements the Court devised in *Huvig*.[16] While the Court did not err when they cited the *Huvig* requirements in *Weber*, their use becomes problematic as the Court uses them in more and more cases which are qualitatively different to *Huvig*. There is a tension between the use of these targeted surveillance safeguards and the bulk surveillance regimes they are used to test. This trend can be seen as the Court attempts to update the *Weber/Huvig* requirements to better reflect the realities of bulk surveillance, ending with the implementation of the 'end-to-end' safeguards in the Grand Chamber judgments of *Centrum* and *Big Brother Watch*.

As the *Weber* minimum requirements test is crucial to the case-law of bulk surveillance, and thus the objective of this chapter, it is worth examining them. First, while they are part of an overall 'in accordance with the law' test they are foreseeability requirements. The overall point of the requirements is that the legislation authorising bulk surveillance is foreseeable to the public who may be subject to it. Although each requirement could be construed as containing some elements of necessity, the Court will not and should not judge them on this. For example, when examining requirement (3), the duration of the interception, the Court is ascertaining whether there is a duration limit set out in the relevant legislation and that this limit is clear to those who may be subject to bulk surveillance. What the Court is not doing is deciding on the permissibility of particular time periods, e.g., whether a six-month limit with

[14] Paul De Hert,, and Gianclaudio Malgieri. "Article 8 ECHR Compliant and Foreseeable Surveillance: The ECTHR's Expanded Legality Requirement Copied by the CJEU. A Discussion of European Surveillance Case Law." *ECLAN Volume, Forthcoming, Brussels Privacy Hub Working Paper* 6, no. 21 (2020).
[15] *Weber and Saravia v. Germany* App no. 54934/00 (ECHR, 29 June 2006) para 95.
[16] *Huvig v. France* (1990) 12 EHRR 528 para 35.

one possible renewal is more proportionate than a three-month limit with indefinite renewals. This is a question of necessity and it is thus inappropriate to answer it as part of a foreseeability test. If tomorrow the UK government published legislation stating that anyone that walked down Oxford Street between 12 - 3pm would be subject to an impromptu strip search in order to prevent terrorist attacks, the implications of walking down Oxford Street during those hours would be foreseeable but this does not mean that the measures are proportionate. Thus, foreseeability requirements are ill-equipped to answer questions of necessity.

6.2.2 Admissibility

The Government in this case submitted that the application was inadmissible as both applicants resided in Uruguay and claimed their communications were intercepted there. Thus, they were not within German jurisdiction. They cited *Banković and Others v. Belgium* in support of this.[17] In this case, the Court rejected the idea of a 'cause and effect' interpretation of jurisdiction in the context of NATO air forces bombing radio stations in Belgrade. Additionally, they submitted that Saravia had failed to exhaust all domestic remedies. The applicants could therefore not claim to be victims of a violation of their convention rights.

The Applicants submitted that Germany had jurisdiction as Weber was a German national. They added that it could not be decisive that the interception was conducted abroad as the State could then avoid their Convention responsibilities by carrying out interferences abroad.[18] They claimed that they had exhausted all domestic remedies and had not been granted redress. They claimed that certain provisions of the amended G 10 Act violated their right to respect for their private life and their correspondence under article 8. Specifically, they complained about five measures of the amended Act;

1. The process of strategic monitoring
2. The transmission and use of personal data
3. Transmission of personal data to the Offices for the Protection of the Constitution and other authorities
4. The destruction of personal data

[17] *Banković and Others v. Belgium* (2007) 44 EHRR SE5.
[18] *Weber and Saravia v Germany* (2008) 46 EHRR SE5 69.

5. The refusal to give notice of restrictions on the secrecy of telecommunications.

One issue covered under this test was whether the interferences were contrary to public international law. Both applicants' communications were intercepted while they were in Montevideo, Uruguay, and applicant two was a Uruguayan citizen. However, the Court ruled that they were not contrary to public international law because the monitoring of wireless telecommunications did not interfere with the territorial sovereignty of foreign states.[19] Additionally the first applicant, who was German, could not rely on an alleged violation of a State's territorial sovereignty in the context of an individual application to the Court. The Court cited *Ocalan*, which held that in order for a respondent State to be tried for violations of international law by breaching the territorial sovereignty of a foreign state the Court requires proof.[20] This proof must be in the form of concordant inferences that the authorities of the respondent state have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign state and therefore contrary to international law.[21]

In regards to the applicants' and the Government's submissions the Court did not find it necessary in the present case to rule on them. Their reasoning for this was that the application was "in any event inadmissible for the reasons set out below",[22]meaning that there was no need to rule on the jurisdiction question as the interference was both in accordance with the law and necessary in a democratic society. This neglecting of a key question of the jurisdiction of these outward facing surveillance systems is a blind spot of the Court which will be returned to later in this chapter.

6.2.3 Weber: A classic Article 8 approach to bulk surveillance

The Court's approach in *Weber* can be seen as being the classic Article 8 approach. The Court first conducted a legality test, checked the interference pursued a legitimate aim and following that performed a necessity test. For the necessity test the Court examined "whether the interferences in question were proportionate to the legitimate aim pursued by each of the impugned provisions in turn", before making an overall assessment of proportionality. The Court held that the provisions of the amended G10 Act which authorise the interception of

[19] *Weber and Saravia v Germany* (2008) 46 EHRR SE5 87.
[20] *Ocalan v Turkey* [GC] (2005) 41 EHRR 45 para 90.
[21] Ibid.
[22] *Weber and Saravia v Germany* (2008) 46 EHRR SE5 72.

telecommunications constituted an interference with the applicants' right to respect for their private life.[23] The Court agreed with the decision of the Federal Constitutional Court that the:

> "transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further interference with the applicants' right under Article 8."[24]

In terms of the foreseeability of the law in the present case, the Court found that the amended G10 Act described precisely "the exact offences for the prevention of which the strategic interception of telecommunications could be ordered."[25] Additionally under section 3(1) and (2) the amended G10 Act indicated which categories of persons were liable to have their telephone tapped. Section 5 of the Act provided a limit on the duration of telephone tapping. The legislative framework also detailed the procedure for examining and using the data obtained, limits and precautions concerning the transmission of data to other authorities and the circumstances in which recordings may or must be erased or tapes destroyed.

The Court thus found that the amended G10 Act framework:

> contained the minimum safeguards against arbitrary interference … and therefore gave citizens an adequate indication as to the circumstances on which the public authorities were empowered to resort to monitoring measures, and the scope and manner of exercise of the authorities' discretion.[26]

As for the 'necessary in a democratic society' test, the Court examined interferences operated under the G10 Framework in five parts; strategic monitoring, transmission and use of personal data, sharing of personal data with other government agencies, the destruction of personal data, and failure to notify the individual under surveillance, finding that the amended G10 act contained adequate and effective guarantees against abuse. The Court was therefore satisfied that the German state:

> "within its fairly wide margin of appreciation in that sphere, was entitled to consider the interferences with the secrecy of telecommunications resulting from the impugned

[23] *Weber and Saravia v. Germany* (2006) App no. 54934/00, para 79.
[24] Ibid..
[25] Ibid, para 96.
[26] Ibid, para 101.

provisions to have been necessary in a democratic society in the interests of national security and for the prevention of crime."[27]

Thus, it is appropriate to treat *Weber* as a starting point for the Court's approach to bulk surveillance as it attempts to apply a set of targeted surveillance requirements to a far broader form of surveillance. This tension will be returned to throughout this thesis as the scope of bulk surveillance grows exponentially.

6.3 Stage 2 (2009-2011): The Innovation of *In Abstracto* Judgments

The cases in stage two both concern the Regulation of Investigatory Powers Act 2000 (RIPA). *Liberty v United Kingdom* concerns the RIPA regime for external surveillance, while *Kennedy* concerns the regime for internal surveillance. In *Kennedy* the Court responded to the twin tensions of the covert nature of surveillance and the ever expanding scope of bulk surveillance by innovating. This innovation was the implementation of *in abstracto* judgments which allowed the Court to bypass the admissibility issue inherent to secret surveillance and fully examine surveillance legislative frameworks.

In *Liberty v United Kingdom* several civil liberties organisations alleged that over a number of years their electronic and telephone communications were intercepted by the Ministry of Defence.[28] The Applicants alleged that in the 1990s the Ministry of Defence operated an Electronic Test Facility (ETF) at Capenhurst, Chesire, the site of modern-day GCHQ. This facility was built to intercept 10,000 simultaneous telephone channels coming from Dublin to London and from there on to the continent. The applicants claimed that between 1990 and 1997 the ETF intercepted all public telecommunications carried on microwave radio between two British Telecom radio stations. These telecommunications included telephone, fax and email communications, and this link carried much of Ireland's telecommunications traffic. During this time period the applicant organisations were in regular phone contact with each other as well as providing legal advice to those who sought their assistance. They alleged that as many of their communications would have passed between the British radio stations and would therefore would have been intercepted by the ETF.[29]

[27] Ibid.
[28] Liberty, British Irish Rights Watch, and the Irish Council for Civil Liberties.
[29] *Liberty v United Kingdom* (2009) 48 EHRR 1 para 5.

In *Kennedy* the applicant had previously been convicted of manslaughter although the safety of his conviction had been publicly questioned by some including Members of Parliament. Following his release from prison the applicant became a campaigner against miscarriages of justice. He alleged that his mail, telephone and email communications were being intercepted. He alleged that this was done with the aim of intimidating him and undermining his business activities. In line with this he sought confirmation from the intelligence agencies and when they refused his requests, he filed complaints with the Investigatory Powers Tribunal (IPT). He requested that his hearing be conducted in public, with mutual disclosure and inspection but this too was refused as the IPT examined his complaints in private and rejected them.[30]

6.3.1 Victim Status

In both cases the Court allowed the applicants to claim to be victims of an interference. In *Liberty,* the Government was prepared to proceed on the basis that the applicants had been victims of an interference with their communications.[31] As the interference in *Kennedy* under Article 8(1) related to the applicant's general complaint about the provision of the Regulation of Investigatory Powers Act 2000 (RIPA), the Court held that the examination for the justification for the interference had to look at the proportionality of the legislation itself, *in abstracto*.[32] While the Court acknowledged its consistent opposition to such review of the relevant law and practice, the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, led the Court to permit general challenges to the relevant legislative regime.

While in *Kennedy* the Court held that the applicant's allegations concerning missing and hoax calls were not sufficient to create a reasonable likelihood of actual interception. Failing the general rule that if an applicant could not prove the alleged actual interception took place the Court would allow for an interception if there was a reasonable likelihood that surveillance measures had been applied.[33] However, as the applicant's allegation concerned that interception was taking place without lawful basis in order to intimidate him, it could not be disregarded that surveillance measures were applied to him or that he was potentially at risk

[30] *Kennedy v United Kingdom* (2011) 52 EHRR 4 paras 19-20.
[31] *Liberty v United Kingdom* (2009) 48 EHRR 1 para 56.
[32] *Kennedy v. UK* (2011) 52 EHRR 4 para 124.
[33] Klass v Germany, Malone v UK, Esbester v UK.

of being subjected to such measures. Thus, the application was admissible as there was an interference with Article 8(1).

6.3.2 Effective Domestic Remedies – The Investigatory Powers Tribunal

While the cases of *Liberty* and *Kennedy* concern differing forms of surveillance, bulk in the former and targeted in the latter, they both concern the same surveillance legislation, and in particular the same safeguards. For example both deal with the Investigatory Powers Tribunal which has been a key safeguard for the UK surveillance regime since its implementation in 2001. However due to the government's acceptance of victim status in *Liberty*, there was no need to ascertain whether the applicants' had exhausted domestic remedies and following the finding of a violation with Article 8 the Court found no need to examine the claim of an interference with Article 13. Thus, while the IPT is present in both cases it is only examined in *Kennedy*.

In *Kennedy*, the Government's objection that the applicant had failed to exhaust domestic remedies led to the Court examining whether the remedy was an effective one available in theory and in practice at the relevant time.[34] This requires the remedy to have been accessible, capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success.[35] The issue with the IPT in Kennedy's case was that his was complaint was a general challenge to primary legislation. If the IPT had upheld this complaint, it had no power to annul any of the RIPA provisions or find any interception arising under RIPA to be unlawful as a result of the incompatibility of the provisions themselves with the Convention.[36] The Court took note of the extensive powers of the IPT to investigate complaints before it and to access confidential information, but did not see clearly their relevance to a legal complaint regarding the operation of a legislative regime. The Court also noted that the IPT is not able to disclose information to an extent, or manner, contrary to the public interest or prejudicial to national security. Thus, it would be unlikely that any further elucidation of the general operation of the surveillance regime under RIPA would result from a general challenge before the IPT.[37] Accordingly the Court considered that the complaint was not inadmissible due to lack of exhaustion of domestic remedies. This inability to place a binding obligation on the executive or to reveal general misuse of the surveillance

[34] *Kennedy v. UK* (2011) 52 EHRR 4 para 109.
[35] *Akdiver v Turkey* (1997) 23 EHRR 143 para 68, *Sejdovic v Italy* (2004) 42 EHRR 360 para 46.
[36] *Kennedy v. UK* (2011) 52 EHRR 4 para 109.
[37] Ibid para 110.

regime under RIPA, and now under the IPA, presents an issue for the IPT as an effective domestic remedy in *in abstracto* complaints. This will be exacerbated by the increasing trend within the ECtHR surveillance jurisprudence to allow for *in abstracto* rulings due to the covert nature of surveillance making victim status exceedingly difficult to prove. The IPT will be returned to later in this chapter in the *Big Brother Watch* judgments.[38]

6.3.3 Addressing necessity and legality jointly

In both *Liberty* and *Kennedy*, the *Weber* requirements were applied to surveillance regimes contained within the same UK legislative framework. As part of the Court's *in abstracto* approach in *Kennedy* the Court stated that it was required to examine the proportionality of the RIPA legislation itself and the safeguards built into the system allowing for secret surveillance, rather than the proportionality of any specific measures taken in respect of the applicant. While in *Liberty* the Court neglected to address the question of necessity, in *Kennedy* the Court explicitly tied foreseeability and necessity together. Thus, the Court held that the lawfulness of the interference with Article 8 "is closely related to the question of whether the 'necessity' test has been complied with in respect of the RIPA regime and it is therefore appropriate for the Court to address jointly the "in accordance with the law and 'necessity' requirements."[39] There appears to be a lack of rigour here as it is not clear whether necessity was considered in both cases. This will be evidenced in the following sections on the application of the *Weber* requirements in each case.

6.3.4 Weber Requirement Application – External Surveillance Regime

In *Liberty* the Court was conducted a truncated form of the *Weber* minimum requirements test by the facts of the case. First the first two requirements of 'nature of offences' and 'categories of people' liable to have their communications intercepted were collapsed into one 'Scope' test. The Court found that the domestic legislation conferred extremely broad discretion for intercepting external communications, namely to intercept "such external communications as are described in the warrant". There was no limit to the type of external communications that could included in such a warrant. Effectively meaning that any person

[38] See chapter 9 on "Review and Oversight in the Investigatory Powers Regime".
[39] *Kennedy v. UK* (2011) 52 EHRR 4 para 155.

who sent or received any form of telecommunications during the period in question could have been intercepted.[40]

This acknowledgment of wide discretion continued into their analysis of the fourth Weber requirement; 'the procedure to be followed for examining, using and storing the data obtained'. There was a wide discretion as to which communications were listened to or read. When the Secretary of State issues an interception warrant they describe what communications should be examined. Even communications coming from an address within the UK could be if necessary in the eyes of the Secretary of State for preventing or detecting terrorism.[41]

From here in the judgment the Court's minimum requirement test collapses into one discussion of the accessibility and foreseeability of the UK regime's safeguards as they were not published in the legislation or in any clarifying documents. The Government argued that publishing information concerning the procedure of the use, storage, destruction and communication of the intercepted data would harm the efficacy of the system. They also argued that it may lead to a security risk. The Court rejected this argument, citing the amended G10 Act in *Weber* as a favourable example of publishing safeguards. Concluding that it was "possible for a state to make public certain details about the operation of a scheme of external surveillance without compromising national security."[42]

The Court concluded that the domestic law at the relevant time did not indicate the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications with sufficient clarity, so as to provide adequate protection against abuse of power. In particular, the legislation did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. Thus, the interference with the applicants' rights under Article 8 were not therefore 'in accordance with the law'.[43] The Court did not examine whether the legislation was in pursuit of a legitimate aim or necessary in society as it had already found a violation in the 'in accordance with law' section. Returning to the lack of

[40] Ibid para 64.
[41] Ibid para 67.
[42] Ibid para 68.
[43] Ibid para 69.

rigour discussed above, this implies that the Court did not consider the *Weber* requirements as part of an examination of necessity, however they did in *Kennedy*.

The *Liberty* judgment shows the emphasis the Court places on the six minimum foreseeability requirements from *Weber and Saravia* in finding that the act in question "allowed the executive an extremely broad discretion in respect of the interception of communications passing between the United Kingdom and an external receiver". In particular, the warrant enabled the executive to intercept "such external communications which could be included in the warrant." The Court's emphasis on the *Weber* requirements as safeguards against excess executive discretion is a recurring theme in this chapter, both in bulk surveillance cases like *Liberty* and targeted surveillance cases such as *Szabo* and *Zakharov*.

6.3.5 Weber Requirement Application – Internal Surveillance Regime

In *Kennedy,* the Court the conducted a full test of the *Weber* minimum requirements as opposed to the truncated version conducted in *Liberty*. For the first requirement, nature of offences liable to give rise to interception, the Court held that these offences do not need to be exhaustive but must be sufficiently detailed. Here the applicants argued that the Act's mention of offences pertaining to 'national security' and 'serious crime' were insufficiently clear. The Court disagreed, stating that national security has been frequently cited in both national and international legislation and is one of the legitimate aims set out in Article 8(2). For 'serious crime' the Court found that the term was defined in the interpretative provisions of the Act itself and what is meant by "detecting" serious crime was also explained in the Act. Thus, while 'national security' is sufficiently clear by itself, 'serious crime' requires clarification for the Court to find it sufficiently clear.[44]

Next, the Court examined the 'category of people' requirement. It found that under the RIPA it was possible for any person in the UK to have their communications intercepted. The Court noted that *Kennedy* was different to the preceding *Liberty* case as *Kennedy* concerned internal rather than external communications. The Court noted an overlap between this requirement and the previous as the relevant circumstances which can give rise to interception provide guidance to the category of people liable to have their communications intercepted. Finally, the Warrant system under RIPA requires the warrant to clearly specify one person as the

[44] Ibid para 159.

interception target in internal communications cases. The warrant can also describe a single set of premises in lieu of this. The Court further noted that indiscriminate capturing of vast amounts of communications is not permitted in internal communications cases.[45] Given that Kennedy's claim concerned internal use of surveillance measures, he could not legally be subjected to indiscriminate surveillance such as bulk surveillance.

Next, the Court examined the duration minimum requirement of the interception. Under RIPA the duration of any telephone tapping is 6 months but is renewable indefinitely by the Secretary of State. Renewal is subject to the Secretary of State satisfying themselves that the warrant remains necessary for the purposes set out in the warrant. The Court observed that in the context of national security and serious crime the general complexity of cases and the numbers of individuals involved will be high. Thus, the Court is of the view that the overall duration of any interception measures will depend on the facts of the investigation in questions. Provided that adequate safeguards exist, the Court doesn't find it unreasonable to leave this matter to the discretion of the relevant domestic authorities.[46]

Following this the Court examined the procedure for examining, using and storing the intercepted data. The Government submitted that under RIPA the intercepting agency could, in principle, listen to all of the collected material. The Court recalled its judgment in *Liberty* wherein the authorities' discretion to capture and listen to intercepted material was considered overly wide. However, the Court acknowledged that this case concerned targeted interception of internal communications rather than bulk interception of external communications. Thus, the fact that the warrant for interception only permits the interception of a specific person's communications and that any captured data which is not necessary for the authorised purposes must be destroyed, constituted a sufficient narrowing of scope.[47]

The Court also looked at the safeguards which apply to the processing and communication of intercepted material. The Government submitted that there was a strict limit on the number of people intercepted data can be disclosed to. It is only disclosed on a need-to-know basis, and that where a summary of the material would suffice it is disclosed instead.[48] Intercepted material, as well as copies and summaries, are stored securely in order to minimise the risk of threat or loss. Access is subject to security clearance and there is a strict vetting process in

[45] Ibid para 160.
[46] Ibid para 161.
[47] Ibid para 162.
[48] Ibid para 163.

place. The Court found that these constituted adequate safeguards for the protection of data obtained. The Court then turned to the circumstances in which the material must or may be destroyed. Under RIPA any intercepted material and associated metadata, as well as any copies, must be destroyed as soon as there are no grounds for retaining them as necessary. Intercepted material must be reviewed at appropriate intervals to confirm that retention is still justified.[49] This discussion points to how the *Weber* requirements can be used in an evaluation of necessity, provided that the legal framework in question contains elements of necessity.

Finally, the Court then found that there was no violation with Article 8. The surveillance measures permitted under RIPA pursued the legitimate aims of protecting national security, preventing crimes and protecting the economic well-being of the country. In regards to foreseeability the RIPA and its associated code of conduct indicated with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communication and destruction of intercept material collected.[50] In regards to adequate safeguards against abuse: the Court held that both in terms of specific safeguards contained within the interception procedures and the more general safeguards offered by the supervision of the Interception of Communications Commissioner, and the review of the IPT, there existed adequate safeguards against abuse.[51] Thus, the potential interferences with the applicant's Article 8 rights were justified under Article 8(2) and there was no violation of Article 8.

6.4. Stage 3 (2016): In Abstracto Reviews of Highly Discretionary Regimes

Decided in the same year *Zakharov v Russia* and *Szabo & Vissy v Hungary* cover similar grounds. They are both *in abstracto* examinations of surveillance regimes, they both deal with surveillance regimes which grant extensive discretion to the executive, and they both deal with internal surveillance with near-unlimited scope. Thus, while neither are explicitly referred to as bulk surveillance cases, they are key to the development of the Court's bulk surveillance jurisprudence. In particular the Court here emphasised the importance of independent, though not necessarily judicial, approval and supervision.

[49] Ibid para 164.
[50] ibid paras 154 – 162.
[51] ibid para 169.

In *Zakharov v Russia* the State Committee for Communications and Information Technologies required telecommunication providers to install equipment on their networks that would allow for direct access to the network without involving specific requests to providers. The applicant, the editor in chief of a publishing company, brought proceedings against the Russian government. The applicant was also the chairperson of an NGO which monitored the state of media freedom in the Russian regions and promoted the independence of the regional mass media, freedom of speech and respect for journalists' rights. Additionally, the NGO provided legal support, through litigation, to journalists.[52] The applicant was subscribed to a number of mobile network operators and in 2003 brought judicial proceedings in the Russian Federation against three mobile network providers. He claimed that equipment had been installed on the mobile networks with the objective of enabling the Federal Security Service to intercept the applicant's telecommunications without prior judicial authorisation.[53]

The applicants in *Szabo & Vissy v Hungary* alleged that Hungarian legislation concerning secret surveillance for national security purposes breached their Article 8 Rights. Both Szabo and Vissy were employees of a non-governmental "watchdog" organisation which publicly criticised the government. Due to this the applicants feared that they would be subject to the legislation. The legislation in question enabled the relevant authority to search and keep a person's home under surveillance, to check their mail, monitor their electronic communications and computer data transmission and make recordings of any data obtained by these methods. Surveillance was authorised by the government minister in charge of justice. The applicants argued that the legislation was in general prone to abuse and pointed to the lack of judicial control as evidence of this.

6.4.1. Victim Status

The Court in *Zakharov* qualified the approach to victim status utilised in *Kennedy* with two conditions. When deciding whether an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, the Court will first consider the scope of the legislation permitting said measures, and second the Court will examine the availability of domestic remedies. In regard to the former the Court will examine whether the applicant can possibly be affected by the legislation. Either because they belong

[52] *Zakharov v Russia* (2016) 63 EHRR 17 para 8.
[53] Ibid para 10.

to a group of persons targeted by the contested legislation or because said legislation directly affects all users of communication services by instituting a system where any and all individuals can have their communications intercepted.[54]In regard to the latter, where the domestic system doesn't afford an effective remedy to the person who suspects that he or she was subjected to surveillance: "widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified."[55]

This approach can be seen to play out in *Szabo* where the Court held that there had been a breach of Article 8 due to three primary reasons. First, although the applicants had not been subjected to surveillance, they could claim victim status by virtue of the mere existence of the legislation. The Court cited the Grand Chamber decision in *Zakharov* which espoused a harmonised approach to victim status based on *Kennedy.* Thus, the Court first examined the scope of the surveillance legislation. As it could not be excluded that they were at risk of being subjected to surveillance measures should the authorities believe that surveillance would be useful in pre-empting or averting a national security threat for example, the Court proceeded to the second part of the *Zakharov* test. This is the availability of domestic remedies, the Court observed that there was no possibility for an individual to lodge a complaint with an independent body against the interception of their communications. Thus, the applicants had victim status.

As it was impossible to evidence that there had been a specific right infringing action against the applicant the Court examined the Russian legislative framework *in abstracto*. While it noted that in general the Court does not consider a claim made *in abstracto* that surveillance legislation contravened the Convention, the fact that the Russian laws didn't provide the applicant with an effective remedy allowed them to. Effectively this meant that the applicant did not need to demonstrate that he is personally at risk of being subjected to secret surveillance in order to achieve victim status. This lines up with the Court's ruling in *Kennedy*.[56] This can be only be seen as a positive in this context. While in other contexts allowing *in abstracto* claims would inundate the Court with applications, the covert nature of surveillance makes this approach a necessity. This is compounded with the fact that intelligence agencies are loathe to notify those who have been subjected to surveillance, making it near impossible to prove even a reasonable likelihood of surveillance being applied

[54] Ibid para 171.
[55] Ibid.
[56] *Kennedy v United Kingdom* (2011) 52 EHRR 4 para 123.

to an applicant. The Court further reiterated *Kennedy* in stating that in cases pertaining to secret surveillance the lawfulness of the interference is closely related to the necessity of the interference. Thus the Court holds that it is appropriate to address the 'in accordance with the law' and 'necessity' requirements jointly.[57]

6.4.2 Addressing foreseeability and necessity jointly

In these cases the Court clarified its approach to addressing foreseeability and necessity jointly first espoused in *Kennedy*. After reiterating the Court's reasoning in *Kennedy* the Court added that "quality of law" in this sense implies that the domestic law in question must not only be accessible and foreseeable in its application, it must also ensure that "secret surveillance measures are applied only when 'necessary in a democratic society', in particular by providing for adequate and effective safeguards and guarantees against abuse."[58] Put this way the Court's logic becomes clear. In order to determine the proportionality of a surveillance regime *in abstracto,* the Court must evaluate the theoretical ability of the safeguards present in the legislation. Put another way, foreseeability is linked here to proportionality in the sense that the safeguards examined under the *Weber* requirements must be foreseeable in order for the court to conduct an assessment of their proportionality. A surveillance regime may contain safeguards which in practice keep the operation of said regime perfectly proportional. If these safeguards are not foreseeable to the Court, and wider public, then the regime will be in violation of Article 8 as the *Weber* requirements will not have been met.

Given that foreseeability is a prerequisite for an assessment of proportionality, this places greater weight on the Court to expand and update the *Weber* requirements to reflect the realities of contemporary bulk surveillance. The *Weber* requirements are often referred to as constituting safeguards and guarantees against abuse, however they omit several key safeguards such as independent authorisation, supervision, notification and domestic remedies. The list of things that need to be foreseeable according to *Weber* is not sufficient to determine the proportionality of a bulk surveillance regime. This approach is placed in clearer terms in the GC judgments of *Big Brother Watch* and *Centrum* which will be addressed in stage 5.

[57] *Zakharov v Russia* (2016) 63 EHRR 17 para 236.
[58] Ibid.

6.4.3 Applying Weber to highly discretionary regimes

The Court's application of the *Weber* requirements to the Russian regime in *Zakharov* focused primarily on the high level of discretion it left the executive at various points of the surveillance process. For example in reference to (1) the nature of offences liable to give rise to an interception. The Russian regime provided that communications may be intercepted in connection with any offence of a medium severity or above which has been already committed, is ongoing or is being plotted. The Criminal code defines an especially serious offence, the highest end of the range, as one for which the Code prescribes a maximum sentence of over three years. This was considered sufficiently clear by the Court but it noted with concern that Russian law allows secret interception of communications for a very wide range of offences, including pickpocketing.

This wide discretion continued in requirement (2); categories of people liable to have their communications intercepted. Interceptions may be ordered in respect of a suspect, an accused or in respect of a person who may have information about an offence or may have other information relevant to the criminal case. The Court noted that they had previously found that interception of one who was not suspected of any offence but could possess information could be justified under Article 8 of the Convention. However, the Court also noted the lack of any clarifications in Russian legislation or case-law as to how the terms "a person who may have information about a criminal offence" and "a person who may have information relevant to the criminal case" were to be applied in practice. Additionally, communications may have been intercepted for information on events endangering Russia's national, military, economic or ecological society. This too was not defined anywhere in Russian Law. In regards to the durations of the interceptions (3), the Court found that the intercepting agency for criminal activities had a procedure for discontinuing interception but the national security agency did not. The Court found no issue with (4) the procedure surrounding the examining, storing and using the intercepted material.

The excess discretion wasn't limited to the executive. The Court found that trial judges had too much discretion with regards to the destruction of the intercepted data. After 6 months of storage, if the person hasn't been charged for a criminal offence the data is destroyed. If they have been charged then the judge decides at the end of the case whether the data is retained or destroyed. Non-relevant data is also retained. The Court found that the lack of requirement to

delete irrelevant data cannot be justified. That the law allows trial judges unlimited discretion as to whether material is destroyed post trials was found to be insufficiently clear.

The Court upheld the complaint. The legal provisions governing the interception of communications didn't provide adequate and effective guarantees against arbitrariness and abuse. This risk was held to be particularly high in a system in which the secret services and the police had direct access to all mobile phone communications. Overall, the Court found that the Russian legal system governing the interception of communication did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of surveillance. This was considered to be particularly stark in the Russian system as the intelligence and the police had direct access to all mobile telephone communications. Several of the *Weber* foreseeability requirements were not met including the circumstances in which public authorities were empowered to intercept communications, the duration of the surveillance, how and what data was to be stored, and destroyed at the end of a trial. The Court found that the law in question did not meet the "quality of law" requirement and was incapable of keeping the relevant interference to what was necessary in a democratic society and there had therefore been a breach of Article 8.[59] Here then we see a repeat of the result in *Kennedy* except for a much larger surveillance operation. This presented an issue as the Court is using the same tests for regimes with ever increasing scope. While *Zakharov* is not considered a bulk surveillance regime by the Court, it is difficult to consider it a targeted surveillance regime considering the scope of the legislation in question.

In *Szabo,* the Court took a rather unstructured approach to their implementation of the Weber requirements test here. Rather than take the formal approach of addressing all of them sequentially in clearly distinct paragraphs, the Court instead examined three of them as part of a larger discussion about authorisation. The Court referenced the *Weber* test through its use in the *Zakharov* case.[60] The Court found the Hungarian answer to requirement (1) sufficiently clear. The reasons for invoking interception were to detect or prevent terrorism and to rescue Hungarian citizens abroad. As to requirement (2) the categories of people liable to have their communications intercepted: it was possible for anyone in Hungary to be subject to the legislation. The legislation in question did not set out categories of people liable to have their communications intercepted. The Court again noted the overlap between the first

[59] Ibid para 304.
[60] *Szabó and Vissy v Hungary* (2016) 63 EHRR 3 para 65.

two *Weber* requirements by drawing on requirement (1) to describe how requirement (2) worked in practice. Proposals for interception must specify either by reference to a specific name or a range of persons. The Court found that the fact that anyone in Hungary could have their communications intercepted was a serious concern as it paved the way to unlimited surveillance. There was no further clarification of how this works in practice in the legislation or accompanying codes of practice. Additionally, the Court found the provision overly broad as there was no requirement to prove connections between persons named in the proposals. Next the Court examined requirement (3) the duration of interception: interceptions could be conducted for a maximum of 90 days but can renewed for another 90 based on necessity. The Court noted that there was no clear rule on whether an interception can be renewed multiple times.

The Court found a violation based on a lack of adequate and effective safeguards against abuse. Notably the Hungarian system was authorised solely by a member of the executive, and proposals themselves had to "specify, either by name or as a range of persons, the person or persons targeted for interception."[61] The Court objected to this statutory language as it could be interpreted as "paving the way for the unlimited surveillance of a large number of citizens." Further the legislation in question made no attempt to clarify this language as it applies to surveillance practices: for example there was no requirement to demonstrate the actual or presumed relation between the person or range of persons considered for surveillance and the prevention of any terrorist threat.[62] This could be construed as the Court requiring reasonable suspicion in order for surveillance measures to be undertaken. The Court was also concerned by the mere possibility that the legislation in question could be construed in order "to enable so-called strategic, large-scale interception"[63], pointing to a potential rejection of wider surveillance practices such as bulk surveillance.

This lines up well with *Zakharov* where the Court stated that interception authorisations must:

> clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such

[61] ibid para 36.
[62] Michael Palmisano. "The surveillance cold war: Recent decisions of the european court of human rights and their application to mass surveillance in the united states and Russia" (2017) 20 Gonzaga Journal of International Law 75-99.
[63] Ibid para 37.

identification may be made by names, addresses, telephone numbers or other relevant information.[64]

At this point in time, there were some that thought that generalised surveillance techniques are inherently at odds with the Convention. Murphy argues that the above quote, combined with the assertion that surveillance authorising bodies must be "capable of verifying the existence of a reasonable suspicion against the person concerned"[65], could be interpreted to mean that generalised surveillance techniques inherently at odds with the ECHR.[66] This was one of the issues that the Court had to address in the subsequent cases of *Centrum* and *Big Brother Watch.* Additionally, while the Court appears to be strictly against the Russian system in *Zakharov*, this is likely due to the near total lack of adequate safeguards in the system for the protection of citizens against abuse.

6.4.4. The importance of supervision

In these cases the Court begins to place emphasis on the importance of independent authorisation in surveillance regimes. In *Szabo* The Court pointed specifically to the lack of judicial control. Under the legislation in question, surveillance for the purposes of protection of national security was authorised by the Minister for Justice. This was done on the condition that the necessary intelligence could not be obtained in any other way. This was the sole test for authorisation. It could be authorised for up to 90 days and could be prolonged for another 90 day period. Once the surveillance was terminated there was no specific obligation on the authorities to destroy it.

The Court stood firmly behind the necessity of judicial control in this case as it offered the best guarantees of independence, impartiality and proper procedure. In a field where abuse is potentially so easy in individual cases and potentially so damaging to democratic society, control by an independent body should be the rule. These independent bodies should be headed by a judge of special expertise. Any alternative to this rule should be treated as an exception which warrants close scrutiny. Correspondingly supervision by a politically responsible member of the executive was held to be inherently incapable of ensuring the requisite assessment of strict necessity.

[64] *Zakharov v Russia* (2016) 63 EHRR 17 para 264.
[65] *Zakharov v Russia* (2016) 63 EHRR 17 para 260.
[66]Maria Helen Murphy, 'Algorithmic surveillance: the collection conundrum' 31 International Review of Law, Computers & Technology 2 p 22.

While the Russian regime in *Zakharov* operated on a system of judicially approved warrants the Court examined evidence to the contrary. In particular by examining documents produced by the applicant which showed that "law-enforcement officials unlawfully intercepted telephone communication without prior judicial authorisation and disclosed the records to unauthorised persons.[67] One such example given was printouts from the internet containing transcripts of the private telephone conversations of politicians. Another submission considered by the Court were news articles describing criminal proceedings against several high-ranking officers from the police technical department. The officers in question were suspected of unlawfully intercepting the private communications of politicians and businessmen in return for bribes from their political or business rivals. The articles in question referred to witness statements "to the effect that intercepting communications in return for bribes was a widespread practice and that anyone could buy a transcript of another person's telephone conversations from the police."[68] The Court was not convinced by the Government's assertion that all interceptions in Russia were performed lawfully on the basis of a proper judicial authorisation, stating that the examples before the Court indicated the existence of arbitrary and abusive surveillance practices, which appeared to be due to the inadequate safeguards provided by law.

6.5 Stage 4 (2018) Applying Weber post-Snowden revelations

The first chamber judgments of *Centrum fur Rattvisa* and *Big Brother Watch* are the first time the ECtHR examined a surveillance regime in the aftermath of the Snowden revelations which revealed the various bulk surveillance regimes operated by Western governments. As such the scope of the surveillance technology in question far outstrips any of the previous cases. These judgments thus contain a number of issues to highlight for this thesis, namely the explicit acceptance of bulk surveillance as being within a state's margin of appreciation, a re-evaluation of the efficacy of the Investigatory Powers Tribunal as an effective domestic remedy, a partial adaptation of the *Weber* requirements, and the consideration of communication data.

In *Centrum* the applicant was a Swedish non-profit organisation with the stated aim of representing clients who claimed that their rights and freedoms under the Convention and under Swedish law had been violated. The applicant communicated daily with individuals,

[67] *Zakharov v Russia* (2016) 63 EHRR 17 para 197.
[68] Ibid.

organisations and companies in Sweden and abroad by email, telephone and fax. These communications were claimed by the applicant to have been particularly sensitive from a privacy perspective. This was due to the nature of its function as an NGO scrutinising the activities of state actors, thus it believed there is a risk that its communications through mobile phones and mobile broadband will have been intercepted and examined through signals intelligence. The applicant brought no domestic proceedings as they contended there was no effective remedy for its Convention complaints in the Swedish legal system.[69]

Big Brother Watch refers to three applications combined. The applicants in each were believed to have had their communications intercepted by UK intelligence services through the use of bulk surveillance programmes. The first two applications were not heard before the domestic courts while the third was heard before the Investigatory Powers Tribunal (IPT). The applicants in this case brought article 8 complaints about two aspects of the British surveillance operation. First the bulk surveillance regime under s.8(4) of the Regulation of Investigatory Powers Act 2000 which allowed the Secretary of State to issue warrants for the Bulk interception of 'external' communications between persons within the UK and those outside it. Second, through intelligence sharing programmes with the US Government the UK Government had access to the near global surveillance of internet communications by the NSA.

6.5.1 Acceptance of Bulk surveillance Practices within Margin of Appreciation

While in the previous stage there was some hope that the rulings in *Szabo* and *Zhakarov* would lead to a rejection of bulk surveillance measures by the Court, the rulings in *Centrum* and *Big Brother Watch* confirm that this was merely wishful thinking. In *Weber* and *Liberty* the Court accepted that bulk interception did not per se fall outside this margin. In *Big Brother Watch* the Court added that while both *Weber* and *Liberty* are now over ten years old, the contemporary threats faced by many Contracting States in that time justified "the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security."[70] The threats cited by the Court included global terrorism, drug trafficking, human trafficking, the sexual exploitation of children, and cybercrime.[71] These threats combined with advancements in technology which have aided terrorists and criminals in evading

[69] *Centrum for Rattvisa v Sweden* (2019) 68 EHRR 2 Para 6.
[70] *Big Brother Watch and Others v. The United Kingdom* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018) para 314.
[71] Ibid.

detection, along with the unpredictability of the routes via which electronic communications are transmitted, justify the use of a bulk interception regime.[72] The Court seems to empathise with States' plight in fighting global terrorism. In addition to it taking a large role in its accepting bulk interception, the Court specifically referred to global terror networks in its ruling on whether the sharing of intercepted data between states was necessary in a democratic society.[73]

6.5.2 Victim Status

In *Centrum* the Court held that the mere existence of secret surveillance measures, or legislation permitting surveillance, could constitute a violation of Article 8. In determining whether there was an interference with the applicant's Article 8 rights the Court examined two aspects. First, the scope of the legislation permitting secret surveillance measures was examined in order to ascertain whether the applicant could possibly be affected by it. The scope of the Swedish legislation potentially affected all individuals sending messages in the Swedish area. Secondly, the availability of remedies at the national level were considered. Individuals who were subject the surveillance were not notified about it and no domestic remedy provided detailed grounds in response to individuals who suspected that their communications had been intercepted. Because of these two facts the Court allowed for an *in abstracto* examination of the legislation.[74]

In *Big Brother Watch:* when considering the admissibility of the complaints made by the applicants in the first and second of the joined cases. There was a question as to whether the lack of exhaustion of domestic remedies would cause these two to be inadmissible. Although a previous finding in *Kennedy* had held that the IPT didn't offer an effective remedy, the UK government argued that the tribunal was designed for complaints of this kind and that its post *Kennedy* jurisprudence showed that it could offer an effective remedy which could have been pursued by the applicants. The Court accepted this but held that the post *Kennedy* jurisprudence had occurred after the applications in question were introduced to the Court.[75] Thus, they were entitled to rely on the finding in *Kennedy*. This presents an issue going forward for applicants challenging the UK surveillance regime as this loophole is now closed.

[72] Ibid.
[73] Ibid para 445 – 446.
[74] Ibid para 171 – 178.
[75] BBW paras 262 – 266.

In addition, it is not clear that the IPT has become an effective remedy since *Kennedy* as they have not gained any new capabilities or powers since that case.[76]

This is problematic on two counts. The Court's reasoning for declaring the IPT an effective domestic remedy is unclear. The ruling in *Kennedy* was that the IPT was not an effective remedy as it had no power to require Parliament to change a law which it viewed as incompatible. As of *Big Brother Watch* the IPT has not gained such a power, and yet the Court now sees it as an effective domestic remedy due to the UK government being willing to listen to the IPT's rulings and legislate accordingly. This policy is not mandated by law and could be changed if the government willed it. This leads into the other reason this ruling is problematic: outside its lack of binding obligation power, the IPT is a flawed institution which is excessively influenced by the executive. This point will be returned to in the chapter evaluating the IPT.[77]

6.5.3 Applying Weber to bulk surveillance regimes - Centrum

With regard to the scope of the legislation the Signals Intelligence Act stipulated eight purposes for which signals intelligence may be conducted. The Court noted that while some of these purposes were generally framed, they are further elaborated on in the preparatory works which is an essential source of Swedish legislation. Thus, the Court found that the scope was adequately indicated.[78] The Court placed more weight on the fact that signals intelligence conducted on fibre optic cables may only concern communications crossing the Swedish border. Communications between a sender and receiver within Sweden may not be intercepted.[79]

The Court held that the legislation on storing, accessing, examining, using, and destroying intercepted data provided adequate safeguards against abuse of treatment of personal data and thus served to protect individuals' personal integrity.[80] While the applicants argued that the procedures in these aspects were regulated in very broad terms, for example there was no general obligation to destroy data. The government in response argued that the Foreign Intelligence Inspectorate was responsible for scrutinising the handling and destruction of data in general. The FII had a mandate to terminate surveillance and order the destruction of data

[76] See chapter 9 on "Review and Oversight in the Investigatory Powers Regime".
[77] See chapter 9 on "Review and Oversight in the Investigatory Powers Regime".
[78] Ibid para 120.
[79] Ibid para 121.
[80] Ibid para 147.

that had been collected in a manner that was incompatible with the permit. The Court rejected the applicant's claim in stating that there were several provisions regulating the situations when intercepted data has to be destroyed, such as when it concerns an unrelated person, anonymous authors or media sources, legally privileged communications, and communications in the context of a religious confession or individual counselling unless there are exceptional reasons for examining said information.[81]

In terms of the duration of the interception the act held that a permit could be granted for a maximum of six months with the possibility of a further six month extension.[82] This extension required a full review by the Foreign Intelligence Court as to whether the necessary conditions for the initial permit were still met. The Court noted that the legislation was not equally clear regarding the circumstances in which interception must be discontinued but stated that the renewal review made up for this shortcoming, as well as the fact that the Foreign Intelligence Inspectorate could decide to halt interception if it was no longer being conducted in accordance with the permit.

The Court's approach in *Centrum* appears to follow the primary trend discussed throughout this chapter where the Court increasingly formulates the traditional three step test of legitimate aim, in accordance with the law, and necessary in a democratic society as a 'minimum safeguards against abuse test'.[83] In line with this the Court throughout *Centrum* referred back to *Zakharov*, often repeating its argumentation word for word.[84] However, *Zakharov* concerned police practices while *Centrum* deals with national security concerns. In this manner the Court seems to provide mostly the same reasoning and safeguards for policing as it does for national security and foreign intelligence. This is problematic as the latter is one in which the Court provides the widest margin of appreciation. Vogiatzoglou provides an example as to this lack of differentiation: In *Centrum* the Court accepted a less authoritative legal provision on cancellation of the bulk surveillance measure than it would in a targeted surveillance case. The reasoning behind this was that "Swedish law is clear on the conditions for expiration and renewal of the interception warrant while a system of review is

[81] Ibid para 145.
[82] Ibid para 23.
[83] Plixavra Vogiatzoglou, 'Centrum for Rattvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy' (2018) 4 Eur Data Prot L Rev 563.
[84] *Big Brother Watch and Others v. The United Kingdom* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018) para 23.

in place." Thus, the foreseeability of the law in bulk surveillance is given even greater weight than in targeted.

6.5.4 Proposed and implemented updates to the Weber requirements in Big Brother Watch

The Court held that there had been a violation of Article 8 in respect of the s.8(4) regime. The Court considered that under this regime the UK government had exceeded the wide margin of appreciation afforded to states to achieve the legitimate aim of protected national security. The Court acknowledged that bulk surveillance was not per se a violation of Article 8 but noted that any operation of it must be compliant with a range of requirements derived from prior case law, namely the *Weber* requirements.[85] The applicants argued that these requirements should be adapted in order to better reflect the realities of bulk surveillance. The proposed updates included a requirement of reasonable suspicion, prior judicial authorisation and subsequent notification of those who had their communications intercepted.[86]

The Court rejected all of the proposed updates but proceeded adapt the *Weber* requirements to better reflect the operation of a bulk interception regime in their own view. The first two minimum requirements – the nature of the offences which might give rise to an interception order and a definition of the categories of people liable to have their communications intercepted – have been categorised by the Court as falling under the title of the scope of application of secret surveillance measures. Here the Court gave its reasoning for changing these two requirements:

> In a targeted interception regime, the nature of the communications to be intercepted should be tightly defined, but once interception takes place it is likely that all – or nearly – all of the intercepted communications are analysed. The opposite will normally be true of a bulk interception regime, where the discretion to intercept is broader, but stricter control will be applied at the selection for examination stage.[87]

The Court here organised the first two requirements into three tests: (1a) whether the grounds upon which a warrant can be issued are sufficiently clear; (1b) whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be

[85] Ibid para 314.
[86] Ibid para 280.
[87] Ibid para 329.

intercepted; and, (1c) whether domestic law gives citizens an adequate indication of the circumstances in which their communications might be selected for examination.[88]

In regards to test (1a) the issuing of warrants under RIPA is the responsibility of the Secretary of State and is subject to their appraisal of necessity and proportionality.[89] First the Court reiterated its view of foreseeability in this context and its opposition to rigid wording in legislation.[90] The Court then referred to its past ruling on the RIPA warrant system for internal interceptions in *Kennedy* where it found the grounds of deploying warrants on the basis of national security and preventing serious crime sufficiently clear.[91] The Court here also found the warrant ground of 'safeguarding economic wellbeing' sufficiently clear.[92] Thus the system of warrants for the bulk interception of external communications was sufficiently clear. Which gave citizens an adequate indication of the circumstance in which and the conditions on which a warrant might be issued.[93]

In terms of test (1b) the Court first acknowledged that the category was wide. Section 8(4) of RIPA permits the Secretary of State to issue a warrant for the interception of external communications. In principle this excludes communications where both of the parties are in the British Islands. The Court acknowledged the confusion surrounding the difference between 'external' and 'internal' communications. Noting that: "even where it is clear that a communication is "internal" … some or all of its parts might be routed through one or more other countries", thereby being at risk of interception.[94] This is expressly permitted under section 5(6) of RIPA, which allows for the interception of communications not identified in the warrant. However, the Court brushed passed this issue. Their justification was that the selection of which bearers to tap in order to conduct bulk interception was not random, rather it was selected based on having the most intelligence value.[95] The Court added that it was desirable for the criteria for selecting bearers to be subject to greater oversight but not necessary due to the nature of bulk surveillance.[96] The Court then noted that in the proceedings for *Liberty* the IPT found that the inclusion of the selectors and search criteria in

[88] Ibid para 330.
[89] Ibid para 331.
[90] Ibid para 332.
[91] Ibid para 333.
[92] Ibid para 334.
[93] Ibid para 335.
[94] Ibid para 336.
[95] Ibid para 337.
[96] Ibid para 338.

the warrants would "unnecessarily undermine and limit the operation of the warrant and would be in any event unrealistic." The Court found no reason to depart from this conclusion.[97] However, they stressed that the search criteria and selectors used to filter intercepted communications should be subject to independent oversight.

Considering test (1c), following the application of the selectors and automated searches, an index is generated. Any material which is not included in the index is discarded. The index may then be examined by an analyst if it meets two criteria: certification by the Secretary of State as to necessity and presence, for the time being, in the British Islands.[98] The Court noted that the certification categories are set out in very general terms. If the "material providing information on terrorism" category is used as an example we find terms which include but aren't limited to: terrorist organisation, terrorists, active sympathisers, attack planning and fund-raising.[99] The Court references the recommendation of the Independent Reviewer of Terrorism Legislation that the purposes for which data was sought should be spelled out by reference to specific operations or mission purposes. The Court agreed that it would be highly desirable for the certificate to be more specific.[100] The Court emphasised that the exclusion of internal communications from interception was an important safeguard. Intelligence services should get a targeted warrant for internal communications. They "should not be permitted to obtain via a bulk warrant what they could obtain via targeted."[101]

In terms of requirement (4), the procedure to be followed for examining, using and storing the data obtained, the Court found that there was not sufficient independent oversight of the inclusion of selectors and search criteria used to filter and search through the intercepted communications. At the same time, the Court noted that these selectors and search criteria do not need to be public or need to be listed in the warrant ordering interception. The Court upheld the conclusion of the IPT (Investigatory Powers Tribunal) in Liberty in stating that including the selectors in the warrant would "unnecessarily undermine and limit the operation of the warrant and be in any event unrealistic."

For the remainder of the *Weber* requirements the Court found the procedures under RIPA to be sufficiently clear. In terms of requirement (3), the duration of the interception. The Court

[97] Ibid para 339.
[98] Ibid para 341.
[99] Ibid para 342.
[100] Ibid.
[101] Ibid para 343.

referenced back to *Kennedy* where it found that the safeguards surrounding the duration of interception were sufficient. In particular, they held up that the duty for the Secretary of State to cancel warrants meant, in practice, that intelligence services had to keep warrants under continuous review.[102] The Court again referenced *Kennedy* under requirement (5), the precautions surrounding communicating intercepted data to other parties, where it was largely satisfied with the safeguards in place. However, the applicants here raised an issue that was not covered in *Kennedy*: the requirement that disclosure and copying be "limited to the minimum necessary for the 'authorised purposes'". The issue surrounded the fact that something may be considered necessary for the authorised purposes if it was "likely to become necessary". This term was not defined in RIPA or the explanatory code or anywhere else. The Court found that the surrounding safeguards were sufficient to stop this from being a real issue as in any case material could only be disclosed to a properly vetted and authorised person.[103] Overall RIPA provided adequate safeguards for the protection of data obtained.[104]

Turning to requirement (6), circumstances under which the intercepted material must be destroyed. This occurs as soon as the intercepted material is no longer necessary.[105] Upon receipt of intercepted content or communications data from an interception, an intelligence agency must specify maximum retention periods based on the nature and intrusiveness of the data in question. This process is automated as much as possible. Retained data is subject to review.[106] According to the 2016 report of the Interception of Communications Commissioner, each interception agency had a different view on what the appropriate retention period was. Retention periods for content ranged from thirty days and one year, retention periods for metadata ranged from six months and one year. The Court thus accepted that, while the periods for which specific datasets could be retained were not in the public domain, in practice retention doesn't last for longer than one year.[107] Additionally, the IPT can examine whether these limits have been observed upon application.[108] Thus, the Court found that the provisions on the erasure and destruction of intercepted material were also sufficiently clear.[109]

[102] Ibid para 360.
[103] Ibid para 368.
[104] Ibid para 369.
[105] Ibid para 370.
[106] Ibid para 371.
[107] Ibid para 372.
[108] Ibid para 373.
[109] Ibid para 374.

6.5.4 Consideration of Communications Data

Crucially to this thesis, the Court in *Centrum* briefly addressed the issue of differing standards of protection for content data and metadata of communications for the first time. The Swedish legislation for signals intelligence seemed to mainly concern the collection of communications data (metadata). The search terms used to intercept this data were less specific than those used for the interception of the content data. However, the Court was convinced by the safeguards in place and the assertions by the Signals Intelligence Committee that the interception of communications data was essential for the proper functioning of the signals intelligence system. Thus, the scope of application for the interception of communications data was sufficiently demarcated.[110] This is key as it shows the Court examining requirements which are not covered by the *Weber* requirements, pointing towards to the need for an expansion or update.

This additional consideration of communications data played a major role in *Big Brother Watch.* Here, the Court took a different stance to its stance in *Centrum*, as the UK government argued that metadata should be exempt from the minimum requirements test. The Court responded that the only difference in treatment between content and metadata was the clause which excluded metadata from the section 16 safeguards surrounding the examination of data, all other safeguards such as authorisation, retention, and destruction applied equally to content and metadata. While the Court saw the utility of metadata to SIAs, they noted as a matter of some concern that the SIAs could search and examine said data without restriction.[111] With regard to the remaining *Weber* requirements the Court found each to be sufficiently clear but the issues of lack of oversight of the entire selection process highlighted above pertaining to requirements 4 and 1(b), and the "absence of any real safeguard applicable to the selection of related communications data for examination" led the Court to hold that the section 8(4) regime doesn't meet the "quality of law" requirement and is thus incapable of keeping the interference to what is necessary in a democratic society. Thus, holding that there was a violation of Article 8 of the Convention.[112] This reliance on a quality of law requirement which is outside the *Weber* requirements to decide the compatibility of the UK surveillance regime highlights the need to update and expand these

[110] *Centrum för Rättvisa v Sweden* (2018) 68 EHRR 2 para 122.
[111] Ibid paras 353 – 355.
[112] Ibid paras 387 – 388.

requirements to better reflect the realities of bulk surveillance. The Court's attempt to do so is evidenced in the GC judgments of *Centrum* and *Big Brother Watch*.

6.6 Stage 5: The Grand Chamber Judgments of Centrum fur Rattvisa and Big Brother Watch

Released on the same day, the GC judgments of *Centrum fur Rattvisa* and *Big Brother Watch* both acknowledge the need to develop the case-law surrounding bulk interception cases.[113] The Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. This 'global assessment' will consist primarily of two components: whether the domestic legal framework contains sufficient guarantees against abuse, and whether the process is subject to "end-to-end safeguards".[114] This global assessment will also have regard to the actual operation of the system of interception, including checks and balances on the exercise of power and the existence or absence of any evidence of actual abuse.

6.6.1 End-to-end Safeguards

In both cases the Court took the position that in order to minimise the risk of the bulk interception power being abused, the process must be subject to "end-to-end safeguards". This means that at the domestic level:

> "an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review."[115]

In the Court's view there are four stages to the bulk interception process: the initial collection or retention, the selection for examination (often via the application of selectors), the examination of selected content/communications data by analysts, and the subsequent data

[113] *Centrum för Rättvisa v Sweden (Grand Chamber)* Application no 35252/08 (ECHR, 25 May 2021) para 254, *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 340.
[114] *Centrum för Rättvisa v Sweden (Grand Chamber)* Application no 35252/08 (ECHR, 25 May 2021) para 274, *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 360.
[115] *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 350.

retention and use and data sharing of the 'final product'.[116] The need for safeguards will be at its highest at the selection for examination stage involving an analyst.[117]

The end product of the Court's deliberation on the need to develop the case law and the need for 'end-to-end safeguards' is an adaptation of the minimum safeguards approach started in *Weber:*

1. The grounds on which bulk interception may be authorised;
2. The circumstances in which an individual's communications may be intercepted;
3. The procedure to be followed for granting authorisation;
4. The procedures to be followed for selecting, examining and using the intercept material;
5. The precautions to be taken when communicating the material to other parties;
6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. The procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[118]

The changes from the *Weber* requirements to the *Big Brother Watch/Centrum* requirements are as such. The first is the change made to *Weber* requirements (1a) and (1b) in the First Chamber *Big Brother Watch* judgment: the nature of offences and categories of people requirements become grounds for authorisation and circumstances in which communications may be intercepted. Requirement (4) has been altered by replacing the "stored" with "selected", this leaves requirement (4) as wholly the selection for examination requirement, as opposed to its previous status as a subsection of requirement 1. The *Weber* requirements pertaining to duration, storage and destruction have been combined into requirement 6 with no difference in practice. The three additions to the *Weber* requirements are (3) the procedure to be followed for granting authorisation, (7) the independent supervision requirement, and (8) the procedures for independent *ex post facto* review. As supervision has always been a part of the wider test for Article 8 compliance in this area, requirement (7) can be seen as a clarification of the Court's previous position. Requirements (3) and (8) are therefore the

[116] ibid Para 325.
[117] Ibid paras 330 – 331.
[118] Ibid para 361.

implementation of the "end-to-end safeguards" into the *Weber* test. In both cases the Court reiterated that this new eight part set of criteria determines whether a domestic law governing a bulk interception regime contains adequate and effective safeguards and guarantees to meet the requirements of 'foreseeability' and 'necessity in a democratic society'.[119]

The Court places considerable weight on the role of independent oversight as part of these "end-to-end safeguards".[120] Each stage of the bulk interception process "should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society"".[121] Given this weight on independent oversight and the above statement that the need for safeguards will be at its highest at the selection for examination stage, it is unclear how the Grand Chamber in *Big Brother Watch* largely found the procedures to be followed for selecting, examining, and using intercept material under RIPA to be adequate.

6.6.2 Applying the new test to Centrum and Big Brother Watch

In applying these new criteria in *Centrum* the Court found that while the main features of the Swedish bulk interception regime met the Convention requirements as to the quality of the law, the regime had three shortcomings.[122] First, regarding requirement 6, the absence of a clear rule on destroying intercepted material which did not contain personal data.[123] Second, with regards to requirement 5, the lack of a requirement to consider the privacy interests of individuals when deciding whether to transmit intelligence material to foreign partner.[124] Finally, with regards to requirement 8, the absence of effective ex post facto review.[125] All three of these shortcomings were not found in the first chamber's assessment of the Swedish legislative regime.[126] The first shortcoming is a direct overturning of the assessment of the first chamber. The second was considered grounds for improvement by the first chamber but was not considered a significant shortcoming. The third was not considered at all by the

[119] ibid para 361.
[120] Ni Loideain N, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment' (*Information Law and Policy Centre,* 2021) <https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/> accessed 08/06/2022.
[121] *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 305.
[122] *Centrum för Rättvisa v Sweden (Grand Chamber)* Application no 35252/08 (ECHR, 25 May 2021) para 369.
[123] ibid para 342.
[124] Ibid paras 326 – 330.
[125] Ibid para 372.
[126] Ibid para 369.

Chamber. Considering that the Grand Chamber now believes such ex post facto review to be a fundamental end to end safeguard this is a significant development.

The Court also found that the UK legislative regime under RIPA had three shortcomings which resulted in a violation of Article 8 ECHR. The first two shortcomings both pertained to requirement 4. The Court took issue with the failure of RIPA to require that categories of selectors be included in warrant applications.[127] The Court also took issue with the lack of any prior internal authorisation of selectors linked to specific individuals.[128] It should be noted that these shortcomings have arguably been accounted for in the Investigatory Powers Act 2016 which uses a system of operational purposes which must be approved as part of the warrant by both the executive and an independent judicial commissioner. Nonetheless this system does have major flaws which will be discussed in the following chapter on UK legislation.[129]

The major shortcoming of RIPA in the view of the Court is that the authorisation of bulk interception was not subject to ex ante independent authorisation. The Court described this as "one of the fundamental safeguards".[130] The UK government has attempted to account for this shortcoming in the IPA through the implementation of a so-called 'double-lock' system wherein prior authorisation is conducted by the Secretary of State with approval from a judicial commissioner. While this is an improvement on the state of affairs under RIPA it is not clear that this so-called 'double-lock' constitutes ex ante independent authorisation given the influence the executive has on the process. This question will be returned to in the following chapter. Again, this is something which was not considered a violation by the first chamber judgment. The first chamber addressed this as part of an overall assessment of supervision and concluded that

> "in view of the pre-authorisation scrutiny of warrant applications, the extensive post authorisation scrutiny provided by the (independent) Commissioner's office and the IPT, and the imminent changes to the impugned regime, it would accept that the

[127] *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 381.
[128] *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 425.
[129] See chapter 8 on "Authorisation and Examination Mechanisms under the IPA 2016".
[130] *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 377.

> authorisation of section 8(4) warrants by the Secretary of State does not, in and of itself, give rise to a breach of Article 8 of the Convention."[131]

Like in *Centrum* the move from *Weber* to these new "end-to-end safeguards" has resulted in a stricter stance by the Court at least in the assessment of aspects of the regimes which were previously excluded from the *Weber* requirements. Still, it isn't clear whether this change has led to an increase in rights protection by the Court on this issue. Like the chamber judgments before them the grand chamber judgments normalise the operation of a bulk surveillance regime, provided adequate safeguards exist.[132] The Court normalises the use of bulk surveillance programmes first by rejecting the privacy advocate's claim that they are categorically disproportionate.[133] Second, the Court normalises these programmes by accepting the governmental case that these programmes are valuable and of vital importance.[134]

Still, there is a flaw in the Court's reasoning present in these eight "end-to-end safeguards" as applied to the present cases. While ex ante authorisation and ex post facto review were treated as fundamental safeguards which require independent supervision and authorities, selection for examination was treated as a lesser requirement which could be addressed at the authorisation stage. This is problematic as there maybe identifying data which only reveals itself at this stage through the use of methods such as data aggregation. Additionally, if the logic justifying bulk surveillance holds, the selection for examination stage is the most intrusive on the individual. While the individual's data may be swept up amidst millions of other terabytes of data, it will only be accessed and viewed by a member of the SIA at the selection for examination stage. The Court's error on this issue evidenced by the Grand Chamber's evaluation of requirement 4 in *Big Brother Watch*, the procedures to be followed for selecting, examining, and using the intercept material. While the Grand Chamber highlighted the above flaws regarding selectors, they overall found that the legislative regime under RIPA for examining said material was sufficiently foreseeable and therefore provided

---

[131] *Big Brother Watch and Others v. The United Kingdom* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018) para 381.
[132] Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa' (*EJIL:Talk!,* 2021) <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> accessed 08/06/2022.
[133] *Big Brother Watch and Others v. The United Kingdom (Grand Chamber)* App nos 58170/13, 62322/14 and 24960/15, (ECHR, 25 May 2021) para 323.
[134] Ibid.

adequate safeguards against abuse.[135] This was an error on the Court's part for both the level of intrusiveness highlighted above, and that the primary safeguard for this stage is set out at the authorisation stage. The level of unaccountable discretion available to analysts at this stage renders the legislation insufficiently foreseeable and incapable of providing adequate safeguards against abuse. As discussed in chapter 4, the use of strong selector and complex queries is where the a large amount of the value, and intrusion, of bulk surveillance comes into play.[136] This does not mean that the new 'end-to-end safeguards' inherently downplay the importance of the selection for examination stage, instead the Court's application in *Big Brother Watch* and *Centrum* blunted the teeth of the safeguards.

This points to the 'end-to-end safeguards' simply being the addition of three new requirements to the *Weber* minimum requirements. Specifically, the new primacy of ex ante authorisation and ex post review when assessing the compatibility of a bulk interception regime with Article 8 ECHR. While the Court acknowledges that there are four stages to the bulk interception process, that each stage should be subject to supervision by an independent authority, and that the need for safeguards is highest at the selection for examination stage. While there is the possibility for similar primacy for the selection for examination stage as written in the new requirement (4) this was not implemented in the *Big Brother Watch* judgment. The Court here did not require independent supervision at the selection for examination stage. Rather the use of warrant descriptors supervised at the authorisation stage was sufficient, provided that they are sufficiently narrow. This ignores the dangers posed by the aggregation of data acquired via interception and other bulk powers where the real intrusion into the individual's Article 8 rights begins: at the selection for examination stage.

6.7 Conclusion

This chapter illustrates the evolution of the Court's approach to bulk surveillance between *Weber* in 2006 and the GC judgments of *Big Brother Watch* and *Centrum* in 2021. There is the growing tension throughout this chapter caused by using targeted surveillance safeguards to evaluate the compatibility of bulk surveillance regimes. Starting in *Weber*, where the Court transplanted the targeted surveillance safeguards from *Huvig*, the Court began a long process of altering these safeguards to better reflect the realities of bulk surveillance. These included combining the first two requirements into one 'Scope' requirement, insisting that

[135] ibid para 391.
[136] See Chapter 4 "Understanding the Harms of Bulk Interception".

communications data must be subject to the same safeguards as content data, and finally the implementation of the 'end-to-end' safeguards. While this evolution is a positive development in the Court's jurisprudence there is still a need for further evolution, specifically to account for the role of aggregation and examination in the operation of surveillance regimes.

In stage two the main evolution was the innovation of *in abstracto* judgments. This is a logical development given the ever increasing scope of bulk surveillance regimes combined with their inherent covert nature makes it nearly impossible for an applicant to prove victim status. However, as this is an abnormality for the Court, it has placed pre-requisites for an *in abstracto* review as of *Zakharov*. When deciding whether an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, the Court will first consider the scope of the legislation permitting said measures, and second the Court will examine the availability of domestic remedies.

In stage three we saw the importance of independent authorisation and supervision. In *Szabo* the Court pointed specifically to the lack of judicial control, and stood firmly behind it as the best guarantee of independence, impartiality, and proper procedure. This was retracted in *Zakharov* however where a system which operated on judicially approved warrants nonetheless was characterised by unlawful interception and misuse of the surveillance regime. This lead to the current position where independent, but not necessarily judicial, authorisation and supervision is required.

The importance of domestic remedies has risen in the Court's approach post-*Zhakarov*. In *Szabo* and *Centrum*, the Court's approach was simple as neither regime had any form of domestic remedy available to those who believed they had been subject to surveillance. Where this becomes more difficult is the *Big Brother Watch* First Chamber judgment which found the IPT to be an effective domestic remedy, directly contravening the Court's judgment in *Kennedy* which held the opposite. The applicants were allowed to claim victim status despite this as they had applied to the Court when *Kennedy* still held. However, considering this loophole is now closed, it raises the importance of evaluating the effectiveness of the IPT as a domestic remedy. The IPT's powers did not change between *Kennedy* and *Big Brother Watch*, with the Court instead citing the IPT's jurisprudence and the executive's willingness

to accept the IPT's judgments. This point will be returned to in the chapter evaluating the IPT.[137]

Stage four contained a number of evolutions in the Court's approach. First, the Court accepted the decision to operate a bulk surveillance regime as being within a contracting parties' margin of appreciation. Second, the Court considered communications data for the first time as part of its evaluation of a surveillance regime, finding that it should be subject to the same level of safeguards as content data. Third, the Court began its process of altering the *Weber* requirements to better fit the realities of bulk surveillance. This process would continue in stage five with the implementation of the 'end-to-end' safeguards.

The final stage of evolution thus far has been the implementation of the 'end-to-end' safeguards test in the GC judgments of *Big Brother Watch* and *Centrum*. While initially appearing to be a new test, upon inspection they are a reformulation of the adequate and effective safeguards against abuse test outlined above. Nonetheless this new formulation presents the Court's emphasis on the presence of safeguards throughout the bulk surveillance process in clearer terms. In addition to the *Weber* foreseeability requirements, the Court requires independent ex ante authorisation, supervision, as well as ex post facto review. As this thesis is concerned with the compatibility of the UK Investigatory Powers Act 2016 with the ECHR, the following chapters will evaluate these safeguards as described in the IPA: namely the Investigatory Powers Commissioner, and the IPT. These chapters aim to show the flaws in these safeguards which may lead to their incompatibility under Article 8 and to show the UK surveillance regime is also lacking in selection for examination safeguards.

[137] See Chapter 9 on "Review and Oversight in the Investigatory Powers Regime".

7. CJEU Case Law on Data Retention and Bulk Acquisition

While the ECtHR has largely failed to reflect the reality of bulk surveillance through its use of a safeguard approach to compatibility, it would be a mistake to assume that the ECtHR is the only source of jurisprudence on the compatibility of bulk surveillance with human rights. Likewise, while the ECHR has predominantly focused on bulk interception as the primary form of bulk surveillance. This does not mean that the remaining powers of Bulk Acquisition (BA), Bulk Equipment Interference (BEI) and Bulk Personal Datasets (BPD) have not been addressed by any court. The European Court of Justice (CJEU) has a rich vein of caselaw on data retention, access, and transmission which provides a rich analysis of a method of bulk surveillance which has not been addressed by the ECtHR, bulk acquisition. This caselaw is most applicable to bulk acquisition as this power under the IPA requires the Secretary of State to issue warrants requiring the transmission of vast amounts of retained data from telecommunications providers.

This chapter aims to incorporate the jurisprudence of the CJEU to outline their approaches to data retention as the bulk acquisition regime under the IPA involves data retention obligations. Specifically, the CJEU's approach to data retention in the cases of *Digital Rights Ireland, Tele2 Sverige, Privacy International* and *La Quadrature*. Each of these landmark cases deals with the compatibility of data retention regimes under EU law. Each of these cases in effect stems from the e-Privacy Directive which concerns the protection of individual's personal data. This chapter begins with providing the context surrounding the CJEU to better understand their approach to data retention before outlining three phases of this caselaw.

Finally, the key takeaways from this case law are applied to bulk acquisition. While the CJEU has taken a stricter stance on data retention initially, and by extension bulk acquisition, their overall approach has softened to something more closely resembling the ECtHR's approach wherein the use of bulk acquisition is permitted for national security purposes subject to meeting adequate and effective safeguards against abuse. Given that the previous chapter on the ECtHR's approach to bulk interception has shown the lack of efficacy of this safeguarding approach, this chapter argues that the protection provided by the CJEU's approach is effectively equal to that provided by the ECtHR. Considering the very different dangers presented by the different forms of bulk surveillance, as discussed in chapters 3 and

4, the futility of limiting potential abuses via safeguarding is shown. This point will be returned to in the following chapter on the UK courts' interpretation of the compatibility of the IPA with both sets of safeguards.

7.1 Introducing the European Court of Justice- *Role of the CJEU*

The jurisdiction of the CJEU stems primarily from Article 19 TEU and Articles 251 – 281 TFEU. Its contribution to EU law has been shaped through the use of Article 19(1) TEU which states that "it shall ensure that in the interpretation and application of the Treaties the law is observed."[1] It is in the name of preserving the rule of law that the CJEU has developed principles of a constitutional nature as part of EU law, which bind the EU institutions and Member States when they act within the sphere of EU law. It is the EU, as interpreter of the Treaties, which adjudicates on the limits of EU competence as against the member states.[2]

As such it has jurisdiction to give preliminary rulings on the interpretation of EU law under Article 267 TFEU and to review the legality of acts of the institutions under Article 263 TFEU. This limits the questions of law which may be referred to the CJEU to two specific areas: the interpretation of the EU treaties and secondary legislation, and the validity of secondary EU legislation.

The CJEU's jurisdiction under Article 267 TFEU is limited in a number of sensitive policy areas. These include the Common Foreign and Security Policy (CFSP) and, importantly, the validity or proportionality of operations carried out by national police, law enforcement authorities, or of the exercise of Member States' responsibilities for the maintenance of law and order and internal security.

It is important to emphasise that the jurisdiction of the CJEU is limited to questions of EU law only, it does not extend to national law at all. In *Ministerio dell'Economica* the CJEU rejected one of the questions referred as it related to rights granted solely by domestic legislation. As it had no basis in EU law, the CJEU had no jurisdiction.[3] However, if the national law in question incorporates provisions or principles of EU law so directly that an independent interpretation by a national court would threaten the uniformity of EU law itself, the CJEU may give a ruling on the interpretation of EU law in such circumstances. There is

[1] Article 19(1) TEU.
[2] Paul Craig and Gráinne De Búrca. 'EU Law : Text, Cases, and Materials'. (OUP 2020) p 62.
[3] *Ministerio dell'Economica e delle Finanze v Paint Graphos Sarl* (C-78-80/08) [2011] ECR I-7611.

no further appeal from the judgments of the CJEU, although member states, EU institutions and other parties may under certain conditions contest a judgment delivered without their being heard, where it is prejudicial to their rights.[4] While the Court generally builds upon its caselaw it does not consider itself bound by a strict system of precedent.[5] The caselaw in this chapter stems from interpretation of the e-Privacy Directive which provides the basis for the CJEU's jurisdiction on the question of data retention.

7.1.1 Advocates General

The CJEU is assisted by Advocates General. The qualifications, method of appointment, and conditions of office of the Advocate General is the same as for the CJEU judges. The duty of the AG is "to make, in open court, reasoned submissions on cases".[6] The AG is a full member of the Court and participates at the oral stage of the hearing but their most important task is to produce a written opinion. This opinion is produced before the Court makes its decision. This written opinion sets out the AG's view of the law and recommends how the case should be decided. While this opinion does not bind the Court it is considered very influential and the Court often follows it. An AG does not have to be involved in every case and are generally not required where the case in question does not raise a new point of law.[7] The AG's opinion is considered here in *Digital Rights Ireland* and *Watson* where the AG took a stronger stance against the dangers of general and indiscriminate data retention than the Court ended up taking.

7.1.2 Differences and Relationship between the ECtHR and the CJEU

There are a number of differences to outline between the ECtHR and the CJEU. The first is that the ECHR has a broader scope as it applies to the 47 Council of Europe States, including the 28 EU Member States while, as mentioned above, the Charter of Fundamental Rights only applies to the EU's institutions and agencies, 28 member states but only when they are implementing EU law. As discussed above the CJEU is responsible for interpreting all EU law, not just the Charter. Individuals have limited access to it, and it is not, strictly speaking a human rights court. Whereas as discussed in previous chapters the ECtHR is a human rights court which individuals have the right to bring cases to once they have exhausted national

[4] Statute (n 205) Art 42.
[5] Anthony Arnull, 'Owning up to Fallibility: Precedent and the Court of Justice' (1993) 30 CMLRev 247.
[6] Article 252 TFEU.
[7] Statute (n 205) Art 20.

remedies. While both courts are legally binding on their respective contracting parties, or member states, the ECtHR's enforcement mechanisms are less powerful than the CJEU's. For example, where a UK court finds that national law cannot be interpreted compatibly with the ECHR, under the Human Rights Act it can recommend that the law be changed. Whereas, prior to Brexit, when a court found that national legislation cannot be interpreted compatibly with the EU charter, under the European Communities Act, it can disapply the law itself. This points to another key difference between the two Courts, as of the writing of this thesis the UK remains a signatory to the ECHR whereas post Brexit the Charter will not apply to the UK.

7.1.3 Influence of retained EU Law Post-Brexit

As of the 31 January 2020 the UK has left the EU. Section 1 of the European Union (Withdrawal) Act 2018 repealed the European Communities Act 1972. However, there was an implementation period for which the completion day was 31 December 2020. The 2018 Act outlines what was to happen during this implementation period and after completion day. Section 4 sets out that any rights, powers, liabilities, obligations, restrictions, remedies and procedures were recognised and available in domestic law by virtue of section 2(1) of the European Communities Act 1972 prior to completion day will continue to be recognised and available in domestic law. Whereas anything that occurs after completion day will not. Likewise, the principle of supremacy of EU law does not apply to any enactment or rule of law passed after completion day but it still applies to the interpretation, disapplication or quashing of any enactment or rule of law made before completion day.

Warby LJ in *R (Open Rights Group Ltd)* outlines the relevance of retained EU law going forward. As it is no longer possible to refer any matter to the CJEU "a UK court must now decide any question as to the validity, meaning or effect of any retained EU law for itself."[8] The general rule is that the court must decide any such question in accordance with any relevant retained case law and any relevant retained general principles. Retained EU case law and general principles are defined here as principles laid down and decisions made by the CJEU prior to the implementation period completion day. Principles laid down and decisions

[8] *R(Open Rights Group Ltd) v Secretary of State for the Home Department [2022]* QB 166, para 23.

made by the CJEU after IP completion day do not bind a UK court but said court may have regard to them.[9]

Thus, the following CJEU case-law, the e-Privacy Directive and the EU Charter remain relevant to this thesis's examination of the Investigatory Powers Act 2016. Furthermore, the e-Privacy Directive and the Charter have the effect given to them by the principle of the supremacy of EU law and take precedence even over primary legislation enacted by the Westminster Parliament.[10]

7.2 The CJEU's Approach to Data Retention

The remaining parts of this chapter outline the development of the CJEU's caselaw on data retention which is a key component of any form of surveillance of communications data but particularly of bulk surveillance. This analysis is divided into three stages. The first stage concerns the landmark case of *Digital Rights Ireland* where the CJEU rejected the Data Retention Directive entirely and took a strong stance on the dangers of surveillance regimes which involved the collection of vast amounts of data. More importantly, the CJEU set out a series of minimum requirements here that data retention regimes must meet to be compliant with EU law. The second stage concerns the joined cases of *Tele2* and *Watson* which concerned whether the ruling in *Digital Rights Ireland* applied to member state legislation which did not implement an EU directive and whether the minimum requirements set out in *Digital Rights Ireland* were all mandatory or if they could be altered by domestic legislation. The CJEU found that the requirements applied to domestic legislation which concerned the retention of data by communication service providers and that these requirements constituted a mandatory minimum in terms of safeguarding. Finally, the third stage concerns the application of *Watson* to the national security context, in the cases of *Privacy International* and *La Quadrature,* finding that while the *Watson* requirements still apply, an imminent and foreseeable threat to national security may justify general and indiscriminate data retention limited to a time period which is strictly necessary.

7.3 Stage 1: Rejecting General and Indiscriminate Data Retention on an EU level

[9] Para 35.
[10] *R (Liberty) v Secretary of State* [2022] 1 W.L.R. 4929 para 36.

The case of Digital Rights Ireland and the joined case of Karntner Landesregierung and Others concerned the 2006 Data Retention Directive.[11] This directive required that providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years. This was required for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. While it did not concern any domestic legislation implementing said Directive, the rejection of this Directive by the CJEU set out a strong opposition against broad scope surveillance practices. While it did not concern bulk acquisition of communications data as per the IPA, it did exemplify the position of the CJEU with regard to the danger of legislative measures which allow for the collection of vast amounts of communications data.

7.3.1 The Dangers of Data Retention

The Advocate General Cruz Villalón considered that the Directive as an instrument of data retention constituted an interference with the right to privacy as set out in Article 8 ECHR and article 7 of the Charter. However, he went further in stating that the Directive constituted "a particularly serious interference with the right to privacy."[12] While he acknowledged that the directive excluded the content of telephone or electronic communications from retention, he emphasised that:

> "the retention in huge database of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitutes a serious interference with the privacy of those individuals, even if they only establish the conditions allowing for the retrospective scrutiny of their personal and professional activities."[13]

Further the Advocate General discussed the surrounding harm and chilling effect this act of data retention could have:

> "The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of

[11] *Digital Rights Ireland Ltd v Minister for Communications* [2015] Q.B. 127.
[12] Ibid para 71.
[13] Ibid para 72.

> citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period."[14]

This particularly serious interference was compounded by the general and indiscriminate nature of the surveillance incurred by the directive's form of data retention.

The Advocate General found that the Directive pursued the perfectly legitimate objective of ensuring that the data collected and retained are available for the purpose of the investigation, detection and prosecution of serious crime.[15] If coupled with the required guarantees, outlined below, the Advocate General found that the Directive could be considered as necessary for achieving that ultimate objective. The Directive itself states that it constitutes "a necessary and effective investigatory tool for law enforcement in several member states, and in particular concerning serious matters such as organised crime and terrorism."[16]

The CJEU, in its ruling, took a very similar approach to data retention as the Advocate General. While the Court stated the data retention required by the Directive constituted a particularly serious interference with Article 7 of the Charter, at the same time, it respected the essence of the right to privacy since it did not concern the content of communications.[17] Likewise, due to the respect the Directive imposed for certain principles of data protection and data security it respected the essence of Article 8 of the Charter. Finally, the Court recognised that the fight against terrorism in order to maintain international peace and security constituted an objective of general interest. As did the fight against serious crime in order to ensure public security.[18] The Court also added that with the growing importance of electronic communication, data retention pursuant to the Directive was a valuable tool for criminal investigations and thus could be considered to be appropriate for attaining the objective pursued by that Directive.[19]

7.3.2 Need for Safeguards

In a similar vein to the ECtHR's test of accessibility, in accordance with law and necessity, the CJEU implements two fold test of an interference being "provided for by law" and its proportionality. In terms of the former, the test must be close to that adopted by the ECtHR

[14] Ibid.
[15] Ibid Para 135.
[16] Recital (9) in the Preamble to Directive 2006/24.
[17] *Digital Rights Ireland Ltd v Minister for Communications* [2015] Q.B. 127 Para 39.
[18] Ibid para 42.
[19] Ibid para 49.

and go beyond a purely formal requirement and consider the quality of the law, or the lack of precision of the law. Regarding the quality of the Directive the Advocate General first raised the issue that while the Directive obligated providers to retain data for access by Member States authorities, it provided that it for the member states themselves to adopt measures to ensure that data retained are provided only to the competent national authorities in specific cases and in accordance with national law.[20]

The Advocate General held that the EU legislature cannot, when adopting an act imposing obligations which constitute serious interference with the fundamental rights of EU citizens, entirely leave to the member states the task of defining the guarantees capable of justifying that interference.[21] This position responds to the defence that the directive only regulates the retention of data, it does not regulate access to the retained data nor their use. It could not do so owing to the division of areas of competence between member states and the EU. The Advocate General's response is that without regulating the conditions of access and use it is very difficult to assess whether the actual interference is constitutionally acceptable.[22] There was nothing to prevent the EU legislature from at least implementing guarantees in the form of principles to guide member states in their attempts to safeguard the access and use of retained data.

The Advocate General then set out a number of guarantees which should have been included by the EU legislature. These include a more precise indication of the criminal activities which are capable of justifying access to retained data than "serious crime."[23] That authorisation to access or use said data should be limited to either a judicial or at least independent authority, or failing that to have requests for access reviewed by such an authority in order to limit the data provided to what is strictly necessary.[24] Other guarantees included the principle of deleting data once no longer required, stricter protections for situations where access may infringe fundamental rights guaranteed by the Charter such as the right to medical confidentiality, notification of the persons concerned of that access, after the elimination of any risk that such notification might undermine the effectiveness of the measures justifying the use of those data. In sum the Court found that the Directive is incompatible with article 52(1) of the Charter and not provided for by law, since the limitations on the exercise of

[20] Ibid para 112.
[21] Ibid para 120.
[22] Ibid para 121.
[23] Ibid para 126.
[24] Ibid para 127.

fundamental rights contained within the Directive were not accompanied by the necessary principles for governing the guarantees needed to regulate the access and use of the data.[25]

With this in mind, the CJEU took another position similar to the ECtHR's. The Court stated that EU legislation that imposes serious interference with rights such as the respect for private life must:

> "must lay own clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so the person whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against unlawful access and use to that data."[26]

The first safeguard set out by the CJEU was that the law should specific the categories of people liable to be monitored. In particular the CJEU highlighted that the Directive did not restrict the retention to data pertaining to a particular time period, particular geographical zone or to a circle of particular persons likely to be involved, in one way or another, in a serious crime. The Directive did not restrict itself to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[27]

The second safeguard concerns the nature of offences which could justify the retention of an individual's data. The Directive failed to lay down any objective criterion by which to determine the limits of access to and use of the data by competent national authorities. The offences used to justify this access of retained data must be considered to be sufficiently serious to justify such a serious interference with the fundamental rights enshrined in articles 7 and 8 of the Charter.[28] The third safeguard concerned objective criteria for limits on the duration of data retention. While the Directive contained a duration of retention limit set between a minimum of 6 months and a maximum of 24 months, it did not state that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.[29]

[25] Ibid para 130.
[26] Ibid para 54.
[27] Ibid para 59.
[28] Ibid para 60.
[29] Ibid para 64.

The fourth safeguard concerned rules relating to the security and protection of data retained by electronic communications providers. The Directive did not lay down rules which were specific and adapted to the vast quantity of data required to be retained under the Directive, the sensitive nature of that data, and the risk of unlawful access to that data[30] The fifth safeguard concerned procedures to ensure the irreversible destruction of data at the end of the data retention period.[31]

The sixth safeguard is judicial overview. The access by competent national authorities to retained data must be dependent on a prior review carried out by a court or independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued.[32] This is linked to the final safeguard, the requirement that the retained data must be retained within the European Union., as it cannot be fully ensured that the judicial overview set out above is applied.[33]

7.3.3 A Rejection of General and Indiscriminate Data Retention

Overall, the Court took a strong stance on data retention by stating that "in light of the important role played by the protection of personal data and the extent and seriousness of the interference with the right caused" by the Directive, the EU legislature's "discretion was reduced, with the result that the review of that discretion should be strict."[34] The Court cited, by way of analogy, the ECHR decision in *S and Marper* in support of this point.[35] In the CJEU's view indiscriminate data retention in the field of law enforcement was not acceptable. Rather data retention must be confined to situations which pose a threat to public security by restricting their scope to a specific time period, geographical zone or specific groups of persons likely to be involved in a serious crime. Access to this retained data should be restricted to what is 'strictly necessary', and limited to the purposes of preventing, detecting and prosecuting precisely defined serious offences. Requests for access should be subject to prior review by a court or independent administrative body. Finally, there should be safeguards that limit the number of persons who have access to the data in line with a specific request. The Court concluded that the EU legislature exceeded the limit imposed by

[30] Ibid para 66.
[31] Ibid para 67.
[32] Ibid para 62.
[33] Ibid para 68.
[34] Ibid para 50.
[35] Ibid para 47, *S and Marper v United Kingdom* (2008) 48 EHRR 1169 para 102.

compliance with the principle of proportionality in light of Articles 7, 8 and 52(1) of the Charter and declared the Directive to be invalid.[36]

It is important to first note that *Digital Rights Ireland* concerns mass communications data surveillance by police within the context of criminal law, rather than bulk communications data surveillance conducted by SIAs in the context of national security previously examined in the ECtHR bulk interception case law. Still, there is significant overlap between the approach by the CJEU in *Digital Rights Ireland* and the ECtHR's approach to bulk interception, specifically with reference to the *Weber* requirements.[37] While *Weber* was not specifically referenced, in their own methodological approach the CJEU found that the Directive did not meet any of these requirements. It is also important to note that this case was concerned with the overall legality of an EU directive rather than a specific implementation of an EU directive into legislation. Thus, side-stepping the member states legitimate aim of fighting serious crime.

Nonetheless, *Digital Rights Ireland* represents a strong stance by the CJEU and a landmark case on data retention. It assigned to the EU a new responsibility to protect human rights, established a strict scrutiny test applicable to EU legislative measures that interfere seriously with human rights and applied rigorous proportionality testing under the Charter.[38] In terms of judicial instructions to member state legislators, the ruling in *Digital Rights Ireland* appeared to instruct legislators to construct a holistic governance system that includes specific safeguards and incorporates extensive checks and balances.[39]

One key difference between the ECtHR and the CJEU at this point in the CJEU's jurisprudence is the willingness of the CJEU to conduct a proportionality test for the Directive instead of focusing on the 'in accordance with the law', or legality, test. However, the Court's approach to proportionality bears a striking similarity to the ECtHR's approach in its bulk interception caselaw. As discussed in the previous chapter, the ECtHR has focused its approach on in accordance with the law safeguards in order to provide adequate and effective

[36] Ibid para 69.
[37] Paul De Hert and Gianclaudio Malgieri, 'Article 8 ECHR Compliant and Foreseeable Surveillance: The ECTHR's Expanded Legality Requirement Copied by the CJEU. A Discussion of European Surveillance Case Law' (2020) 6 Brussels Privacy Hub Working Paper.
[38] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39 European Law Review 834
[39] ibid

safeguards against abuse. Here, we see the CJEU move these safeguards to a question of proportionality and take a stronger stance on the need for strict scrutiny of these general and indiscriminate measures.

Three key questions stem from the ruling in *Digital Rights Ireland*. First, what is the level of interference caused by the retention of communications data as opposed to the retention of content data. While the Court ruled that general and indiscriminate retention of any data is not permitted, they also stated that the retention of communications data respects the essence of the right to privacy in a way that the retention of content does not. As this thesis has shown, communications data can be hugely intrusive on not just the right to privacy but also to the rights of freedom of expression and freedom of assembly. The second question concerns the fact that *Digital Rights Ireland* concerns an EU directive, do the *Digital Rights Ireland* requirements apply to domestic legislation which does not implement an EU directive such as the Data Retention Directive. The third question concerns the nature of the *Digital Rights Ireland* requirements, do they constitute a set of mandatory, minimum safeguards, or are they more akin to guidance on the part of the CJEU to legislation which employs data retention measures.

7.4 Stage 2: The Application of the Digital Rights Ireland to National Legislation

The joint cases of *Tele2 and Watson* provide answers to these questions. Following *Digital Rights Ireland*, the UK enacted the Data Retention Investigatory Powers Act 2014 (DRIPA), which sought to restore the powers contained in the Directive. It enabled the Secretary of State to adopt measures that would require public telecommunications services to retained all traffic and location data for a period up to 12 months. This could be done without any prior authorisation.

7.4.1 General and Indiscriminate Retention of Communications Data

Tele2 and Watson is an important decision on the legal status of communications data.[40] In both the referred cases the national legislation in question required the general and indiscriminate collection and retention of data related to the identity and location of the user, the identity of the recipient and the time and date of the communication. The specific data in question included the name and address of the user, telephone number of the caller, the

[40] Isabella Buono and Aaron Taylor. "Mass surveillance in the CJEU: forging a European consensus." *The Cambridge Law Journal* 76, no. 2 (2017): 250-253.

number called and an IP address for internet services. That data makes it possible to identify the person with whom a subscriber or user has communicated, by what means, the time of the communication as well as the place from which the communication took place.[41] General and indiscriminate was here defined as a legislation measure providing for the retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systemically and continuously, with no exceptions.[42]

The Court acknowledged that such "data, taken as a whole is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."[43] This is a significant difference from the CJEU's approach in *Digital Rights Ireland* where the Court drew a distinction between metadata and the content of communications. The Court here referred back to the Advocate General's position that this data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive than the actual content of the communications.[44]

The Advocate General first outlined the usefulness of general data retention obligations in the fight against serious crime. Such obligations, in contrast with targeted surveillance measures, enables law enforcement authorities to "examine the past" by consulting retained data.[45] As general data retention obligations relate to all communications effected by all users, without requiring any connection whatsoever with serious crime. The usefulness of general data retention in the fight against serious crime lies in its "limited ability to examine the past by consulting data that retraces the history of communications effected by persons even before they are suspected of being connected with a serious crime."[46]

Next the Advocate General examined the disadvantages of general data retention obligations. In line with the advantages, the disadvantages arise from the fact that the vast majority of the data retained will related to persons who will never be connected in any way with serious crime. The Advocate General here cited the opinion of Advocate General Cruz Villalón in *Digital Rights Ireland.* That the use of such data makes it possible "to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his

[41] Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2015] Para 98.
[42] Ibid Para 97.
[43] Ibid Para 99.
[44] Ibid.
[45] Ibid Para 178.
[46] Ibid Para 181.

private life, or even a complete and accurate picture of his private identity."[47] In the individual context "a general data retention obligation will facilitate equally serious interference as targeted surveillance measures, including those which intercept the content of communications."[48] The CJEU's decision in *Watson* is a reversal of their position on communications data in *Digital Rights Ireland*. Here both the Court and the Advocate General took the position that the intrusion caused by the retention of communications data is at least at a similar level to content data. This is an important factor to consider in terms of the compatibility of bulk acquisition, the justification for which is dependent on communications data being considered less intrusive than content.

7.4.2 Does Digital Rights Ireland Apply to Member State Legislation?

The Court's answer to this question came down to an examination of Article 15(1) of Directive 2002/58 which states that member states may adopt "legislative measures to restrict the rights and obligations provided for in article 5, article 6, article 8(1), (2), (3) and (4), and article 9" of that same Directive. Article 15(1) cited "providing for the retention of data" as one possible measure that could be implemented.[49] Article 15(1) further stated that the objectives that these measures must pursue such as safeguarding national security overlap substantially with the objectives pursued by the activities referred to in article 1(3) of that Directive.[50] Despite this the legislative measures mentioned in Article 15(1) could not be excluded from the scope of the Directive for otherwise that provision would be deprived of any purpose. Further, the wording of Article 15(1) necessarily presupposed that the national measures referred therein fall within the scope of that directive, since it "expressly authorises the member states to adopt them only if the conditions laid down in the Directive are met."[51]

The specific scope of the Directive extended to a legislative measure that requires such providers to retain traffic and location data, since to do so necessarily involves the processing, by those providers, of personal data.[52] The scope also extended to a legislative measure relating to the access of the national authorities to the data retained by the providers of electronic communications services.[53] The protection of confidentiality guaranteed in

[47] Ibid. Para 253, *Digital Rights Ireland* paras 72-74, 27, 37.
[48] Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2015] Para 254.
[49] Ibid para 71.
[50] Ibid para 72.
[51] Ibid para 73.
[52] Ibid para 75.
[53] Ibid para 76.

article 5(1) of the Directive applies to all measures taken by all persons other than users, whether private persons, or bodies or state bodies. Thus, a legislative measure that required providers of electronic communications services to grant national authorities access to data retained by those providers, concerns the processing of personal data by those providers and that processing falls within the scope of that Directive.[54]

This position lines up well with the arguments of the Advocate General in this same case, that such obligations do not go beyond the bounds of what is strictly necessary, provided that they are accompanied by certain safeguards concerning access to the data, the period of retention and the protection and security of the data.[55] The Advocate General specifically took the reading of *Digital Rights Ireland* which meant that a general data retention obligation goes beyond what is strictly necessary where it is not accompanied by stringent safeguards. He emphasized that nothing in *Digital Rights Ireland* which implied that general data retention obligations inherently go beyond what is strictly necessary. The Advocate General then referenced the ruling in *Schrems* as confirmation of this interpretation[56] where, in that case, the Court did not find that the regime in question went beyond what was strictly necessary because it authorised the general retention of data. Rather it was because "of the combined effect of the possibility of such generalised retention and the lack of a safeguard in relation to access aimed at reducing the interference to what was strictly necessary."[57] This is another important factor when discussing the compatibility of bulk acquisition with retained EU law. As of the writing of this thesis the e-Privacy directive remains implemented in UK law via the Privacy and Electronic Communications Regulations.

7.4.3 The Mandatory Nature of the Digital Rights Ireland Requirements

In light of the positive answer to the first question, the Court emphasised that the Directive seeks to ensure full respect for the rights set out in articles 7 and 8 of the Charter.[58] To this end the Directive contains specific provisions designed to offer the users of electronic communications services protections against risk to their personal data and privacy that arise from new technologies and the increasing capacity of for automated storage and processing of data.[59] These include ensuring the confidentiality of communications effected by means of

[54] Ibid para 78.
[55] Ibid para 193.
[56] Ibid para 203.
[57] Ibid para 204.
[58] Ibid para 82.
[59] Ibid para 83.

a public communications network and publicly available electronic communications services, and the confidentiality of the related traffic data.[60] As per article 5(1) confidentiality is taken to mean that as a general rule any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. While the previously mentioned Article 15(1) allows for member states to introduce exceptions to this principle, that provision must be interpreted strictly, in accordance with the court's settled case law.[61]

Article 15(1) provides the legitimate objectives which allow for the legislative exception to the confidentiality principle: "to safeguard national security-that is, state security-, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized used of the electronic communications system."

To this end the Court set out that in order to fulfil the requirements of Article 15(1) the national legislation must lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards. The legislation in particular must indicate in what circumstances and under which conditions a data retention measure may, as a preventative measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary.[62] The Court cited *Digital rights Ireland* here.[63] The Court next outlined the substantive conditions to limit data retention to what is strictly necessary. While these criteria may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue to meet objective criteria. These criteria must establish a connection between the data retained and pursued objective. The extent to which of that measure and the effect on the public must be shown.

The Court went further here in setting out these requirements. Legislation which seeks to impose data retention measures must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect link, with serious criminal offences, and to contribute in one way or another to fighting serious crime or preventing a serious risk to public security. These limits can include using a geographical

[60] Ibid para 84.
[61] Ibid para 89, Probst v mr.nexnet GmbH (Case C-119/12) [2013] CEC 913.
[62] Ibid para 109.
[63] *Digital Rights Ireland Ltd v Minister for Communications* [2015] Q.B. 127para 54.

criterion where the authorities consider, on the basis of objective evidence, that there exists a high risk of preparation for serious offences in a given area.[64]

The Court concluded by stating that the ruling in *Digital Rights Ireland* must apply to national legislation which does not implement an EU directive. Specifically, that article 15(1) of Directive 2002/58 read in the light of articles 7, 8, 11 and 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime provides for the general and indiscriminate retention of all traffic and location data and registered users relating to all means of electronic communication. *Digital Rights Ireland* does lay out a set of minimum requirements for data retention.

The Court's reasoning in *Watson* lines up well with the conclusions of the Advocate General who concluded that the mandatory safeguards stemming from *Digital Rights Ireland* are no more than minimum safeguards aimed at limiting the interference with the rights enshrined in the e-Privacy directive and articles 7 and 8 of the Charter to what is strictly necessary. As such:

> "a national regime which includes all of those safeguards may nevertheless be considered disproportionate, within a democratic society, as a result of a lack of proportion between the serious risks engendered by such an obligation, in a democratic society, and the advantages it offers in the fight against serious crime."[65]

This implies that meeting all the *Digital Rights Ireland* safeguarding requirements may not matter if the use of the power to retain data is disproportionate to its aim. For example, the use of a general data retention obligation in order to stop petty crime would be disproportionate no matter how clearly stated and subject to limitations it is. A general and indiscriminate surveillance measure would necessarily be narrowed to either a targeted or a bulk surveillance measure by applying the *Digital Rights Ireland* minimum safeguards and the *Watson* safeguards requiring an objective evidence-based link between serious crime and the public who will be subject to the surveillance measure. This leaves open the question of what is proportionate to use for the stated aim of national security in the view of the CJEU.

[64] Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2017] Q.B. 771 Para 111.
[65] Ibid para 262.

7.5 Stage 3: Applying *Watson* to a National Security Context *Privacy International* and *La Quadrature*

Privacy International is the first of two cases examined here that place the CJEU's ruling in *Watson* in the context of national security. Handed down on the same day as the second case, *La Quadrature*, *Privacy International* concerned the acquisition and use by UK SIAs of bulk communications data under section 94 of the Telecommunications Act 1984. Notably, it did not concern the retention of said communications data thus differentiating it from the DRIPA 2014 regime addressed in *Watson*, just the access to data which was already retained by telecommunications providers in the course of their economic activity. The questions in the joint cases addressed in *La Quadrature* came down to whether article 15(1) of the Directive 2002/58 must be interpreted as precluding national legislation which imposes on general data retention obligations for the purposes of national security.[66] The referring courts in question were unclear as to the possible impact of the right to security enshrined in article 6 of the Charter on article 15(1) of the Directive 2002/58.[67] In addition the referring courts asked whether the interference with Articles 6 and 7 of the Charter by general data retention obligations could be justified in the context serious and persistent threats to national security.[68]

7.5.1 Applying Watson to a national security context and the bulk acquisition of communications data

The IPT, as the referring court, found that the bulk acquisition of communications data was essential to the work of SIAs in countering serious threats to public security, particularly terrorism, espionage and nuclear proliferation.[69] The respondents argued that the bulk acquisition regime was not within the scope of the Treaty and the Directive and is only subject to ECHR.[70] The IPT found that while the regime appeared to be compliant with Article 8 ECHR, the *Watson* requirements appeared to go beyond the ECHR requirements. In that they required prior authorisation (except in the case of emergencies), a restriction on non-targeted access to bulk data, subsequent notification for those affected and the retention of all data within the EU.

[66] La Quadrature du Net v Premier Ministre (C-511/18) [2021] 1 W.L.R. 4457 para 81.
[67] Ibid para 85.
[68] Ibid.
[69] Privacy International v Secretary of State [2021] 1 W.L.R 4421 para 17.
[70] Ibid para 49.

The IPT thus made a request to the CJEU for a preliminary ruling clarifying the extent that the *Watson* requirements could apply to where the bulk acquisition and automated processing techniques were necessary to protect national security. The IPT emphasised that if they did apply to measures meant to safeguard national security, they would frustrate them and in doing so place national security at risk. Specifically, the Tribunal noted that the requirement for prior authorisation for bulk acquisition could undermine the intelligence services' ability to tackle threats to national security. The impracticability of such a requirement and the treaty implications that an absolute bar on the transfer of data outside of the EU would have.[71]

In regards to the first question, by relying on the logic set out in *Watson* the CJEU found that Article 15(1) of the Directive 2002/58 necessarily presupposes that the national legislative measures referred to therein fall within the scope of that Directive, since it expressly authorises the member states to adopt them only if the conditions in the Directive are met.[72] Following on from this the Court addressed the claims that applying the *Watson* requirements would frustrate the powers of bulk acquisition and in doing so undermine national security. The Court rephrased this question as whether article 15(1) of the Directive 2002/58 is to be interpreted as precluding national legislation enabling a state authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.[73]

The Court stated that article 15(1) does not preclude such national legislative measures where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the fighting of crime. Member states may adopt legislative measures providing for the retention of data for a limited time period justified on one of those grounds.[74] However, the Court emphasised that the national security exception under the Directive should not become the rule[75] and that member states are not permitted to adopt such legislative measures to restrict the scopes of the rights and obligations provided for the in the Directive unless they do so in accordance with the general principles of EU law, including the principle of proportionality. The Court reiterated its stance in *Watson* that, such limitations to the fundamental rights of privacy and

[71] Ibid para 29.
[72] Ibid para 38.
[73] Ibid para 50.
[74] Ibid para 58.
[75] Ibid para 59.

data protection must be limited to what is strictly necessary.[76] In order to satisfy the requirement of proportionality the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse.[77]

While the CJEU acknowledged the importance of the objective of safeguarding national security, stating that it goes beyond that of the other objectives referred to in article 15(1) of Directive 2002/58: combatting crime, serious crime, and the safeguarding of public security. Subject to meeting the requirements laid down in article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing serious interferences with fundamental rights than those which might be justified by those other objectives.[78]

However, this does not mean that legislation justified by national security aims can go beyond what is strictly necessary. Legislation entailing interference with the fundamental rights enshrined in articles 7 and 8 of the Charter must meet the requirements stemming from the CJEU's caselaw, in particular *Digital Rights Ireland* and *Watson.*[79] The Court reiterated that these requirements apply equally to legislation does not require the retention of communications data but only that providers provide access to retained data.[80] National legislation requiring providers of electronic communications services to disclose communications data to SIAs by means of general and indiscriminate transmission, such as the bulk acquisition regime in this case, exceeds the limits of what is strictly necessary and cannot be considered to be justified in a democratic society.[81] This is confirmation by the Court that while the national security context may justify more invasive measures this does not mean that the *Digital Rights Ireland* requirements do not apply. This further pushes the level of protection provided by the CJEU's approach to that provided by the ECtHR's approach where increasingly invasive measures are justified by national security but kept in place by a set of minimum safeguards.

[76] Ibid para 66.
[77] Ibid para 68.
[78] Ibid para 75.
[79] Ibid para 76.
[80] Ibid para 77 – 80.
[81] Ibid para 82.

7.5.2 La Quadrature - An Exception for National Security Threats

At the same time the CJEU made an exception for general and indiscriminate data retention in the face of genuine and foreseeable national security threats. The Court set out that the objective of safeguarding national security had not yet been specifically examined by the Court in judgments interpreting Directive 2002/58. The Court set out that article 4(2) of the EU Treaty provides that national security remains the sole responsibility of each member state.[82] The importance of this objective goes beyond that of the other objectives referred to in article 15(1) of the Directive 2002/58 such as combatting crime in general, serious crime and safeguarding public security. The objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.[83] Thus the Court found that article 15(1) does not, in principle, preclude a legislative measure which implements general data retention obligations on service providers for a limited period of time, as long as there are sufficiently solid grounds for considering that the member state concerned is confronted with a serious threat to national security.[84]

> "Even if such a measure was applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection … with a threat to the national security of that member state, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection."[85]

The Court next set out the required safeguards for such a general data retention obligation to be limited to what is strictly necessary. The Court here did not explicitly reference the requirements set out in *Digital Rights Ireland* and *Watson*. Rather the Court emphasised the duration of the obligation to be limited to what is strictly necessary, although the duration may be renewable, and that the authorities which issue such general data retention obligations be subject to review by either a court or an independent administrative body whose decision is binding. This review must be done with the aim of verifying that a situation of a national security threat exists and the conditions and safeguards which must be laid down are observed.[86]

[82] La Quadrature du Net v Premier Ministre (C-511/18) [2021] 1 W.L.R. 4457 para 134
[83] Ibid para 136.
[84] Ibid.
[85] Ibid para 137.
[86] Ibid para 139.

7.5.3 Automated Analysis of Communications Data

Another question considered by the CJEU in *La Quadrature* was whether article 15(1) must be interpreted as precluding national legislation which requires providers of electronic communications services to implement, on their networks, measures allowing the automated analysis and real-time collection of traffic and location.[87] The referring court noted that the aim of that processing is to detect links that might constitute a terrorist threat.[88] The CJEU noted that the automated analysis in question corresponds to a screening of all the communications data retained by providers of electronic communications. This screening is carried out by the providers at the request of the competent national authorities according to parameters set by the latter. The CJEU termed this to be the undertaking on behalf of the competent national authority of general and indiscriminate processing.[89]

The CJEU took the same position as done with the question of general and indiscriminate data retention obligations above. That the particularly serious interference constituted by general and indiscriminate processing can only meet the principle of proportionality in situations where a member state is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary.[90]

7.5.4 Further Consideration of Communications Data

The CJEU in *La Quadrature* drew a distinction between IP addresses and other forms of communications data. IP addresses are generated independently of any particular communication and mainly serve to identify the natural person who owns the equipment from which an Internet communication is made. Therefore, provided that only the IP addresses of the source of the communication are retained and not the IP addresses of the recipient, these IP addresses do not disclose any information about third parties who were in contact with the person who made the communication. Thus, IP addresses are considered to be less sensitive than other forms of communications data.[91] However, the Court also considered that IP addresses may be used to track a user's entire online activity and thus to create a detailed

[87] Ibid para 169.
[88] Ibid para 170.
[89] Ibid para 172.
[90] Ibid para 177.
[91] Ibid para 152.

profile of the user to be produced created a serious interference with the fundamental rights of the Internet user enshrined in Articles 7 and 8 of the Charter.[92]

In their account of the balance between the rights and interests at play in this case, the CJEU accepted the utility of IP address retention to law enforcement. Where a criminal offence is committed online, the IP address might be the only means of investigating the identity of the user who committed the offence. The CJEU highlighted child pornography and sexual exploitation offences as a problem which the retention of IP addresses may be necessary to address.[93] Thus despite the reality that general and indiscriminate retention of all IP addresses of all natural persons who own equipment permitting access to the Internet would catch those with no connection to such offences, a legislative measure providing for the general and indiscriminate retention of only IP addresses does not appear to be contrary to article 15(1) of the Directive 2002/58. Provided that such measures are subject to strict compliance with the substantive and procedural conditions which should regulate the use of that data.[94] The Court took the same approach with regard to the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems.[95]

The CJEU's view here is similar to what can be seen in *Ministerio Fiscal.* This request for a preliminary ruling arose after Spanish police asked the investigating magistrate in a case of the theft of a mobile phone and a wallet for access to data. The specific data requested was for the data identifying the users of telephone numbers activated with the stolen telephone during a period of twelve days prior to the theft. The magistrate rejected the request on the basis that the circumstances given rise to the criminal investigation didn't constitute a 'serious' offence. The question of the threshold of seriousness of offence above which an interference with fundamental rights was justified, such as access to data retained by electronic communications services by national authorities, was then referred to the CJEU. In their ruling the Court referred back to *Watson* where only serious crime can justify this kind of access to retained data due to the serious interference with.[96] Likewise where the interference is not serious access is capable of being justified by the objective of preventing, investigating, detection and prosecution of 'criminal offences' more generally. The Court

[92] Ibid para 153.
[93] Ibid para 154.
[94] Ibid para 155.
[95] Ibid para 157 – 159.
[96] Proceedings brought by Ministero Fiscal [2019] 1 W.L.R. 3121 para 55, Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2017] Q.B. 771 para 99.

then applied this proportionality test to the subject interference and found that it did not consider access to the data to be a particularly serious interference. This was due to analysis of the identifying nature of the data in question. The data in question only enabled the SIM card or cards activated with the stolen mobile phone to be link during a specific period of time with the identity of those the SIM card owners. This data alone would not allow the Spanish police to make precise conclusions to be drawn concerning the private lives of the persons whose data is concerned. This data would require cross-referencing with communications data and location data to do so. This case shows how the CJEU's approach to proportionality can allow for the variable level of restrictiveness based on the level of intrusion.

7.6 Applying the CJEU's Data Retention Caselaw to Bulk Acquisition

Returning to the focus of this thesis, what utility can the CJEU's caselaw provide for the protection of human rights against the dangers of bulk surveillance. The first question following from this is whether this caselaw, and as such the requirements as per *Watson*, can be applied to bulk acquisition. The answer to this question is clear, the requirements stemming from CJEU caselaw apply to bulk acquisition. These requirements stem from e-Privacy Directive which as of the writing of this thesis remains accessible and applicable in domestic UK law as retained EU law. The scope of that Directive extends to legislative measures which require electronic communications providers to retain data, and those which require electronic communications providers to provide access or transmission of data. Thus, bulk acquisition of communications data under the IPA falls within the scope of the e-Privacy Directive.

The second question is whether bulk acquisition should be considered to be general and indiscriminate. The four cases examined here are concerned with general and indiscriminate data retention obligations. However, it isn't clear whether bulk acquisition as per the IPA should be considered to be general and indiscriminate. In *Tele2 and Watson* this was defined as a legislation measure providing for the retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systemically and continuously, with no exceptions.[97] Bulk acquisition is narrower in scope

[97] Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2017] Q.B. 771 Para 97

than this and yet it wider in scope than targeted retention, the bulk acquisition regime under the IPA is far narrower than the regime challenged in *Watson* under DRIPA.

Another way of defining general and indiscriminate is as a term describing a data regime which does not meet the requirements required to keep said retention proportionate with the Directive 2002/08 and the Charter. Given the nature of the *Watson* requirements necessarily limits the scope of data retention regime it is not possible for a general and indiscriminate regime to meet them. Therefore, these requirements must be applicable to regimes which are broader in scope than a targeted regime but narrower in scope than a general and indiscriminate regime. Thus, the *Watson* requirements must be applicable to bulk acquisition as otherwise they would lose all practical effect. This question, along with the question of the UK Courts' overall approach to retained EU law post Brexit, will be returned to in the following chapter on the UK jurisprudence on the Investigatory Powers Act 2016, specifically the divisional high court cases of *Liberty v Secretary of State*.

Thus, it can be argued that bulk acquisition under the IPA is within the scope of the e-Privacy directive and thus subject to the minimum requirements set out by the CJEU in *Digital Rights Ireland* requirements. These can be summarised as follows:

1. Categories of people liable to be monitored.[98]
2. The nature of offences that could trigger surveillance.
3. Limits on the duration of monitoring.
4. Rules for the security and protection of data retained by providers.
5. Rules for the irreversible destruction of the data at the end of the data retention period
6. Oversight by an independent but not necessarily judicial body.

Watson added a further requirement to these, that legislation that seeks to impose data retention measures must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect link, with serious criminal offences, and to contribute in one way or another to fighting serious crime or preventing a serious risk to public security. These limits can include using a geographical criterion where the authorities consider, on the basis of objective evidence, that there exists a high risk of preparation for serious offences in a given area.[99] These safeguards appear initially provide a

[98] Digital Rights Ireland para 58 – 59, Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2017] Q.B. 771para 105

[99] Ibid para 111.

higher standard of protection than the ECtHR's *Big Brother Watch* safeguards discussed in the previous chapter. However, the context the Court is operating in *Watson* and *Digital Rights Ireland* is the context of serious crime, not national security.

In the national security context, as per *Privacy International*, the Court stated that article 15(1) does not preclude such national legislative measures where this constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence and public security, and the fighting of crime. Member states may adopt legislative measures providing for the retention of data for a limited time period justified on one of those grounds.[100] However, the Court emphasised that the national security exception under the Directive should not become the rule[101] and that member states are not permitted to adopt such legislative measures to restrict the scopes of the rights and obligations provided for the in the Directive unless they do so in accordance with the general principles of EU law, including the principle of proportionality. The Court reiterated its stance in *Watson* that, such limitations to the fundamental rights of privacy and data protection must be limited to what is strictly necessary.[102] In order to satisfy the requirement of proportionality the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse.[103] The Court found in *La Quadrature* that the 2002/58 Directive read in light of the Charter precluded legislative measures which provided for the general and indiscriminate retention of communications data. However, the Court added that where the member state concerned was confronted with a serious threat to national security that was shown to be genuine and present or foreseeable, that member state could utilise such general and indiscriminate measures for a period that was limited to what was strictly necessary. This period could be extended if the threat persisted. The CJEU also took this approach about the obligation placed on service providers to screen for national security threats generally and indiscriminately.

This ruling places the CJEU's approach in a very similar place to the ECtHR's wherein there is a margin of appreciation afforded to member states in the context of national security

[100] Ibid para 58.
[101] Ibid para 59.
[102] Ibid para 66.
[103] Ibid para 68.

provided that they provide adequate and effective safeguards against abuse. This raises questions as to the protection that these requirements can provide against the harms incurred by bulk acquisition and bulk surveillance more generally. If the safeguards provided by the ECtHR do not adequately reflect the reality, and hence the dangers, of bulk surveillance, then what is the possible utility of a set of similar safeguards which are limited to a specific type of bulk surveillance.

These stages have also seen the CJEU change its mind in regard to how intrusive the collection of communications data is. The CJEU's view on the intrusive nature of communications data has shifted throughout the caselaw examined here. In *Digital Rights Ireland* the CJEU took the position that the surveillance of communications data does not disrupt the essence of the right to privacy in the same way that the surveillance of content does. This would line up well with the UK SIAs justification for the use of bulk acquisition within the UK.

However, in *Watson* the Court went back on this position, stating that communications data when taken as a whole is liable to allow very precise conclusions as to the private lives of those persons whose data was collected. In this sense communications data became equal to content data in terms of intrusion. This was further complicated by the Court's delineation of IP addresses and civil identities from communications data in terms of intrusiveness in *La Quadrature*. Here the CJEU held that despite the reality that the general and indiscriminate retention of all IP addresses and civil identities of the users of electronic communications systems would catch those with no connection to serious crime, it did not appear to be contrary to Article 15(1) of the e-Privacy Directive. Providing, of course, that the use of that retained data is subject to strict compliance with substantive and procedural safeguards. Thus, the Court's position on the key justification of bulk acquisition, that communications data is necessarily less intrusive than content, is unclear. The UK court's answer to this question will be discussed in the next chapter.

7.7 Conclusion

This chapter has sought to incorporate the CJEU's caselaw into this thesis' analysis to complement the ECtHR caselaw examined in the previous chapter. While this initially appeared to be a stronger source of human rights protection against the dangers of bulk surveillance than the ECHR, in reality the CJEU has provided another set of safeguards by which to test the compatibility of bulk surveillance. However, these safeguards are narrower

in application than the ECtHR's. While the ECtHR has only addressed bulk interception thus far, the *Big Brother Watch* safeguards can be applied to the other bulk powers, even if these safeguards do not adequately reflect the realities of these other powers. The CJEU safeguards can only be applied to powers which require electronic communications providers to retain data, and those which require electronic communications providers to provide access or transmission of data. Thus, while it applies to bulk acquisition under the IPA it does not necessarily apply to bulk interception, bulk equipment interference or bulk personal datasets.

Next there is the issue that the CJEU safeguards are in effect quite similar to the ECHR safeguards. It isn't clear that the protection provided by these safeguards is higher than the safeguards under *Big Brother Watch*. Finally, while the CJEU does not explicitly invoke a margin of appreciation for a member state's decision to utilise bulk surveillance for national security purposes. The rulings in *Privacy International* and *La Quadrature* make clear that in the national security context the CJEU views the operation of regimes which may be wider in scope than bulk surveillance are, in principle, permitted. As bulk surveillance operates only within the national security context, it again isn't clear that the CJEU caselaw can provide much more protection than the ECtHR's against the harms of bulk surveillance.

8. Authorisation and Examination Mechanisms under the IPA 2016

As the primary approaches of the ECtHR and CJEU are a test for adequate and effective safeguards against abuse, an evaluation of the safeguards present in the IPA regime is required. Discussion in the prior chapter on the ECtHR largely centred around foreseeability requirements as part of this evaluation of safeguards. With the establishment of the Grand Chamber *Big Brother Watch* and *Centrum* judgment, in addition to the *Weber* foreseeability requirements, the Court requires independent ex ante authorisation, supervision, as well as ex post facto review for compatibility with the ECHR under Article 8. The primary ex ante authorisation safeguard in the IPA 2016 is the so-called "double-lock" system. It is worth noting that the major shortcoming of the UK legislative regime prior to the IPA, RIPA, in the view of the Court was that the authorisation of bulk interception was not subject to ex ante independent authorisation. The Court described this as "one of the fundamental safeguards".[1] The so-called "double-lock" system is the UK government's attempt to account for this shortcoming.

Before a bulk powers warrant can be issued, the Secretary of State's decision to issue it must be approved by a Judicial Commissioner.[2] The Judicial Commissioner will review the Home Secretary's conclusions as to whether the warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved.[3] The Judicial Commissioner will also review the Home Secretary's conclusion as to whether each of the operational purposes specified on the warrant is a purpose for which the use of said power is, or may be, necessary.[4] It should be noted that these operational purposes are one of the very few examination safeguards present within the IPA. This so-called 'double-lock' system is the primary ex ante safeguard present in the IPA. The system was highlighted in the GC judgment of *Big Brother Watch*:

> "The issuing of the warrant is subject to prior approval by a Judicial Commissioner, who must apply the principles of judicial review (the so-called "double-lock"). The Judicial Commissioner must therefore consider for himself or herself questions such

[1] Ibid para 377.
[2] IPA 2016 s 140.
[3] Ibid s 140(1).
[4] Ibid para 4.13.

> as whether an interference is justified as being proportionate under Article 8(2) of the Convention."

As alluded to in the previous chapter, the 'double-lock' system raises a number of issues which this chapter analyses. First, the chapter evaluates what the appropriate role of the judiciary is in this area, finding that while the JCs are likely to assess the necessity and proportionality of the warrant, there is a risk that without a sufficiently strict standard of review they will simply offer a thin veneer of legality. This leads into a discussion of the standard of review that the JCs are likely to apply. While the discourse around the IPC centred primarily on what standard of review the Judicial Commissioners would apply, this chapter shows how there is not much difference between the two proposed standards of review. Rather the issue from an ECHR compatibility stand point comes from how the standard of review and deference is indeterminate from an outside perspective.

The standard of review is likely to be a substantive review based on two contextual factors: the subject matter of the warrant and the level of deference afforded to the decision maker under review. This then requires an analysis of the likely deference that JCs will afford the executive when approving warrants and the structural and institutional factors which influence this deference. Finally, the chapter combines these factors into a discussion of how the JCs are likely to evaluate warrants. In sum this chapter forms a thorough evaluation of the Judicial Commissioners as a key safeguard of the bulk surveillance regime under the Investigatory Powers Act 2016.

8.1 Judicial Commissioners – The Appropriate Role of the Judiciary

Within the separation of powers Parliament, the executive, and the courts each have their distinct and largely exclusive domain. Parliament has a legally unchallengeable right to make whatever laws it thinks right. The executive carries on the administration of the country in accordance with the powers conferred on it by law. The courts interpret these laws and see that they are obeyed.[5] In practice, however, there is a complex interplay between these organs of the state. This requires:

> the courts on occasion to step into the territory which belongs to the executive, not only to verify that the powers asserted accord with the substantive law created by Parliament, but also, that the manner in which they are exercised conforms with the

[5] R. v Secretary of State for the Home Department Ex p Fire Brigades Union [1995] 2 AC 513, 567.

> standards of fairness which Parliament must have intended. Concurrently with this judicial function Parliament has its own special means of ensuring that the executive, in the exercise of delegated functions, performs in a way which Parliament finds appropriate.[6]

Nonetheless, within the current organisation of government branches the executive finds itself in an unusually powerful position. The separation of powers is "highly incomplete and enables the executive government to arrogate power to itself through its effective control of the sovereign legislature."[7] The power of Parliament to hold the executive to account, while influential in certain aspects, is arguably inadequate for its stated purpose. This dominance of the executive has led to a paradox where the more powerful the executive the greater the need for effective systems of accountability to guard against and deal with abuses of power.[8] Yet this dominance of the executive acts as an obstacle to such accountability. This view fits into the Parliamentary Decline theory which has been popular in political science circles for over a century, although as Flinders and Kelso point out it may be problematic in its simplicity.[9] In light of this arrangement, people have increasingly looked to the judiciary, as well as other institutions, to fill this accountability deficit.[10] This is stated most succinctly by Sedley:

> "It is the executive … which is subject to public law controls. That is because executive government exercises public powers which are created or recognised by law and have legal limits that it is the courts' constitutional task to patrol."[11]

This issue of executive accountability is compounded in the context of holding the intelligence agencies to account. SIAs are accountable, first, to the Government, who are in turn accountable to Parliament with all the caveats outlined above. Next the SIAs are accountable to Parliament through the Intelligence and Security Committee, whose efficacy as an accountability measure is limited by the covert nature of the SIAs, and the perceived lack of independence of the ISC from the Government.[12] This is the context within which the judiciary attempt to provide effective oversight of the executive under the IPA. The primary

---

[6] Ibid para 567.
[7] Mark Elliott and Robert Thomas, *Public Law* (4th edn, OUP 2020) p 493.
[8] Ibid.
[9] Matthew Flinders and Alexandra Kelso, 'Mind the Gap: Political Analysis, Public Expectations, and the Parliamentary Decline Thesis' (2011) 13 British Journal of Politics and International Relations 249.
[10] ibid p 494.
[11] Stephen Sedley 'Judicial Politics' (2012) 34 London Review of Books 15 (http://www.lrb.co.uk/v34/n04/stephen-sedley/judicial-politics).
[12] Ibid p 478.

roles available to them under the IPA are the Investigatory Powers Commissioner and Judicial Commissioners, discussed in this chapter, and the Investigatory Powers Tribunal, discussed in the chapter that follows.

Given the constraints outlined above, what is the appropriate role for the judiciary in this process? By its very nature the granting of these warrants is a risk-based analysis. The SIA presents their argument for the presence of a national security threat and their proposed response to it in the form of a warrant. The Secretary of State then determines whether this warrant is necessary and proportionate to the threat. Following this, the Judicial Commissioner reviews the Secretary's decision. This will include questions of necessity and proportionality. An issue that Judicial Commissioner must consider when addressing the question of necessity is the institutional competence of the judiciary to review the Home Secretary's decision. When addressing the question of proportionality, an issue for the Judicial Commissioner to address is whether the executive's accountability to the public precludes the judiciary from taking too stringent a stance on national security matters. Institutional competence and democratic accountability are relevant to the broader question whether it is consistent with the separation of powers for a Judicial Commissioner to determine whether a warrant should be issued or not.

It has long been held that risk analysis in the context of national security is the purview of the executive.[13] Both in terms of democratic accountability and institutional competence, it is not seen as appropriate for the courts to override the executive in this context. The executive is subject to political accountability to Parliament and in turn to the electorate, whereas the judiciary are subject to neither. Likewise, the executive has access to resources and expertise in this field that the judiciary has no access to, such as the classified information of the SIAs. However, in line with the ruling in the *Belmarsh Detainees* case it would seem that the Court sees an appropriate role in this national security process. While it admitted that it would be inappropriate for the court to supplant the executive in determining what constitutes a risk to national security, it held that where human rights were engaged the court had a role in determining the proportionality of the response. In other words, while the court deferred to the executive on the question of risk assessment, and the necessity of the measures, the court did rule on the proportionality of the measures. This distinction between the assessment of

[13] *Secretary of State for the Home Department v Rehman* [2001] UKHL 47, [2003] 1 AC 153, *R (Lord Carlile of Berriew QC) v Secretary of State for the Home Department* [2014] UKSC 60.

risk and the appropriate response is key to understanding how the JCs are likely to operate as they are both key questions within the authorisation procedure for issuing a warrant under the IPA.

Belmarsh can be seen as an emphatic rejection of the idea that the courts should adopt a completely hands-off approach to matters of executive decision making in pursuit of national security aims:

> It is no longer perceived to be the exclusive province of the executive. When national security is involved, non-justiciability is now replaced with a variable intensity review in light of the overall context of the case, where the courts will strive to determine the constitutionally appropriate degree of restraint in that context.[14]

In short, the idea of national security representing a judicial no-go area was replaced by a "more flexible and pragmatic test of deference".[15] This is key to understanding the approach that will likely be taken by the Judicial Commissioners in their review of the Secretary of State's decision-making.

The House of Lords did not sustain the highly stringent approach set out in *Belmarsh* in subsequent cases. An example is *Gillan*, where the House took a highly deferential position on the use of stop and search powers under the Terrorism Act 2000.[16] Lord Hope, in addition to granting deference to the Secretary of State on the usage of stop and search powers under the TA, was willing to grant significant discretion to the police in the use of said powers because they "need to be free to decide when and where the use of the procedure is to be authorised."[17] *Gillan* is a good comparator for the JCs as both concern the use of investigatory, preventative powers which engage Article 8 ECHR in a national security context. One notable difference between the two is that the stop and search powers under the PTA had no form of judicial authorisation. Rather the stop and search orders are authorised by the Assistant Commissioner of the Metropolitan Police and confirmed by the Secretary of State. This is effectively oversight of executive action by the executive, as will be discussed

[14] Aileen Kavanagh, 'Constitutionalism, Counterterrorism, and the Courts: Changes in the British Constitutional Landscape' (2011) 9 International Journal of Constitutional Law 172. p 178.
[15] Jeff King, 'The Justiciability of Resource Allocation' [2007] 70 Mod. L. Rev. 198 p 224.
[16] T Scaramuzza, 'Judicial deference versus effective control: the English courts and the protection of human rights in the context of terrorism' [2006] 11(2) Coventry Law Journal 2, 10.
[17] R (on the application of Gillan) v Commissioner of Police for the Metropolis [2006] UKHL 12, at [51].

later. Nonetheless, this lack of judicial oversight did not factor into the Court's view on the Article 8 presence of adequate and effective safeguards test.

While *Belmarsh* can be seen more as a 'one-off' than a 'landmark' for the House of Lords, their stance in *Belmarsh* has filtered down to the lower courts.[18] Specifically, the Administrative Court[19], Special Immigrations Appeals Commission (SIAC)[20] and the Proscribed Organisation Appeal Commission (POAC).[21] These courts and tribunals who review the decision-making of the executive in the national security context at first instance have taken a much more intense level of judicial scrutiny.[22] As the JCs also review the decision-making of the executive in this context, they may take a similarly intense level of scrutiny in their operation.

Control orders, and their successors in TPIMs, serve as a good comparison for the process of judicial authorisation discussed under the IPA. TPIMs are coercive orders which may be imposed on an individual if the Secretary of State considers it necessary to do so in the interests of national security, so they are pursuing the same public interest as bulk powers warrants under the IPA. Control orders, TPIMs and interception warrants are preventative rather than punitive measures. However, it should be noted that it is not a perfect comparison. The restrictions under Control Orders and TPIMs were far more intrusive for the individual than the use of bulk surveillance powers. While all three engage human rights considerations under Article 8, one such legal challenge to control orders came via Article 6 ECHR in *Re MB* and other procedural challenges to the control order regime under TA.[23]

In the first instance judgment of *Re MB* Sullivan J concluded that the control order review hearings as set out in the Prevention of Terrorism Act 2005 violated Article 6(1) ECHR.[24] He interpreted said Act as only requiring the court to "review whether the Home Secretary's

[18] Adam Tomkins, 'National Security and the role of the court: a changed landscape?' [2010] L.Q.R. 2010, 126(Oct), 543-567, p 544.
[19] R. (on the application of Secretary of State for the Home Department) v Bullivant [2008] EWHC 337. (Admin), Secretary of State for the Home Department v NN sub nom. Secretary of State for the Home Department v GG [2009] EWHC 142 (Admin).
[20] Al Jedda v Secretary of State for the Home Department, SIAC, judgment of April 7, 2009.
[21] Secretary of State for the Home Department v Lord Alton of Liverpool [2008] EWCA Civ 443; [2008] 1 W.L.R. 2341.
[22] Adam Tomkins, 'National Security and the role of the court: a changed landscape?' [2010] L.Q.R. 2010, 126(Oct), 543-567, p 544.
[23] This was not the only potent legal challenge, there was also Secretary of State for the Home Department (Appellant) v. JJ and others (FC) (Respondents) [2007] UKHL 45 on the intensity of COs, and Secretary of State for the Home Department v AF and others [2009] UKHL 28 on CO disclosure.
[24] [2006] EWHC 1000 (Admin).

decision that the statutory conditions were met was flawed at the time of the decision, and not also at the time of the review hearing".[25] In practice this meant that the court's supervisory role was severely limited, as the court had to judge the Home Secretary's decision without regard to any subsequent information or explanation from the individual concerned or their special advocate. Control orders were made by the executive and, while prior judicial authorisation was required, the order could be made without notice to or consultation with the individual concerned.[26] Thus, with the addition of the low standard of proof and possibility of closed sessions, Sullivan J issued a declaration of incompatibility with Article 6. In particular, he cited a "procedure which is uniquely unfair",[27] and accused it of seeking to apply a "thin veneer of legality".[28] The judicial authorisation procedure under the IPA faces a similar danger of simply applying a thin veneer of legality to the actions of the executive. While bulk surveillance warrants contain less restrictions and obligations when compared to control orders, they are implemented without regard to any individual who might fall within their remit. There is also a similarly low standard of proof of possible intelligence value. Due to how the double-lock functions, JCs are effectively limited to reviewing the Home Secretary's decision at the time of the decision.

The case was then appealed in *Secretary of State for the Home Department v MB*, which concerned the standard of judicial review which should be applied in such control order hearings.[29] Section 2 of the Prevention of Terrorism Act stated that:

(1) The Secretary of State may make a control order against an individual if he
    a. Has reasonable grounds for suspecting that the individual is or has been involved in a terrorism-related activity;
    b. and considers that it is necessary, for purposes connected with protecting members of the public from a risk of terrorism, to make a control order imposing obligations on that individual

Under a section 3(10) hearing the court was required to determine three matters:

1. Is the Secretary's decision under s2(1)(a) flawed?

[25] Stuart Macdonald, 'The role of the courts in imposing terrorism prevention and investigation measures: normative duality and legal realism' (2015) 9 Criminal Law and Philosophy 265, p. 278.
[26] Ibid.
[27] *Re MB* [2006] EWHC 1000 (Admin) para 85.
[28] Ibid para 103.
[29] Adam Tomkins, 'National Security and the role of the court: a changed landscape?' [2010] L.Q.R. 2010, 126(Oct), 543-567, p 549.

2. Is the Secretary's decision under s2(1)(b) flawed?
3. Is each of the obligations imposed by the control order necessary?

Regarding the first question the Court of Appeal ruled that the court must be robust. "Whether there are reasonable grounds for suspicion is an objective question of fact. We cannot see how the court can review the decision of the Secretary of State without itself deciding whether the facts relied upon by the Secretary of State amount to reasonable grounds."[30] Here is a key difference with the system of review under the PTA and the double-lock system under the IPA. The IPA does not specify a "backward-looking" precondition that requires proof of certain acts. The preconditions are all "forward-looking" matters of judgment, like necessity and proportionality. This is in contrast to similar measures like Control Orders and TPIMs, where proof of involvement in terrorism-related activity is a precondition. As there is no requirement that the Home Secretary must be satisfied of certain facts before being able to issue the warrant, there is no decision about the establishment of certain facts for the JC to review. This is important because the Home Secretary's decision about necessity and proportionality must have some factual basis. But the legislation doesn't (expressly) call for a review of the Home Secretary's findings of fact. It could be argued that the assessment of necessity will involve some assessment of the findings of fact, as the more speculative the factual basis, the harder it will be to claim necessity. Nonetheless this is indeterminate and thus not foreseeable from outside the IPC.

The JCs cannot directly decide whether the facts relied upon by the Secretary of State amount to reasonable grounds to authorise a bulk surveillance warrant. The scope of their review is restricted by the legislation to reviewing how the Secretary of State made their decision.

Regarding the second question, on the necessity of the order, the court invoked "the customary test of proportionality."[31] It should be noted that this does not necessarily equal a more stringent standard of review. As will be discussed later in this chapter, there are circumstances which can reduce a proportionality review to a rationality review. The court then deferred to the executive in stating that the Secretary is better placed than the court "to decide the measures that are necessary to protect the public against the activities of a terrorist suspect".[32] This was immediately qualified by the court's view on the third question:

[30] *Secretary of State for the Home Department v MB* [2006] EWCA Civ 1140 para 60.
[31] Ibid para 63.
[32] Ibid para 65.

> Notwithstanding such deference there will be scope for the court to give intense scrutiny to the necessity for each of the obligations imposed on an individual under a control order, and it must do so.[33]

The judicial authorisation regime under the IPA is not identical to the control orders regime but some key insights can be drawn from this comparison. One key difference is that it is not within the JC's remit to question the fact-based grounds for issuing a warrant, as the Home Secretary is better placed to decide on the merits. Under the IPA, the JCs review the Home Secretary's decisions as to whether the interception warrant is necessary and whether the conduct it authorises is proportionate to what is sought to be achieved. As demonstrated above, in the national security context there is an appropriate role for the judiciary in providing oversight. However, the questions of appropriate standard of review and appropriate deference remain open. These will be addressed in the following sections.

Assessing the facts presented to the Secretary of State by the SIAs remains outside of this role but the JCs are likely to examine the necessity and proportionality of the proposed bulk surveillance measures as a response. At least in the human rights context this does not seem to constitute a breach of the separation of powers. The judiciary in this context are not supplanting the executive's decision with their own, they are simply assessing whether the executive's decision infringes human rights. In this way the implementation of Judicial Commissioners is a positive development as the judiciary are in the best position to provide accountability to the actions of the executive in the form of the Secretary of State and the SIAs themselves. One worrying consideration is that although there is an appropriate role in the warrant authorisation process under the IPA without an intense standard of review there is a danger that – echoing *Re MB* above – the judicial authorisation will apply a thin veneer of legality to the actions of the executive. The following section aims to reconcile this danger by outlining the likely standard of review the JCs will employ.

8.2 Judicial Commissioners – Standard of Review

As discussed in the previous chapter, discourse surrounding the establishment of the IPC centred around whether the JCs would apply *Wednesbury* standard of review or a proportionality standard of review. While the question of whether there is an appropriate role for the judiciary in this context is not in contention, the question of the level of the test the JC

[33] Ibid.

will apply in reviewing the Secretary of State's decision to approve the warrant remains unclear. This is a false dichotomy however, as 'proportionality' is a variable standard, and in national security contexts is not all that different to *Wednesbury* unreasonableness. This section will show that the standard of review will be based on a contextual analysis of the subject matter of the warrants, such as the national security context the JCs operate in.

First, it is useful to set out what is meant by the *Wednesbury* and proportionality tests. While *Wednesbury* was set out in *Wednesbury*, Lord Diplock provided a succinct explanation of the notion of irrationality in *GCHQ*:

> By 'irrationality' I mean what can now be succinctly referred to as 'Wednesbury unreasonableness'. It applies to a decision which is so outrageous in its defiance of logic or accepted moral standards that no sensible person who had applied his mind to the question to be decided could have arrived at it. Whether a decision falls within this category is a question that judges by their training and experience should be well equipped to answer … 'Irrationality' by now can stand upon its own feet as an accepted ground on which a decision may be attacked by judicial review.[34]

The wording of *Wednesbury* unreasonableness being akin to a decision which is 'so outrageous in its defiance of logic or accepted moral standards' is quite stringent. In *Tameside* Lord Denning adopted similar wording in stating that "no one can properly be labelled as being unreasonable unless he is not only wrong but unreasonably wrong, so wrong that no reasonable person could sensibly take that view."[35] This strictness is justified by the courts as owing to the supervisory function of the judiciary in the application of judicial review. In *Brind* Lord Ackner summed up the test as:

> If no reasonable minister properly directing himself would have reached the impugned decision, the minister has exceeded his powers and thus acted unlawfully and the court in the exercise of its supervisory role will quash that decision.[36]

This strictness in application of *Wednesbury* can lead to difficult and sensitive situations, such as in *Smith* which concerned the discharging of four individuals from the armed forces on the basis of their homosexuality. The policy which discharged them had been extensively

[34] *Council of Civil Service Unions and Others v Minister for the Civil Service* [1985] AC 274 paras 410 – 411.
[35] *Secretary of State for Education and Science v Tameside Metropolitan Borough Council* [1977] AC 1014.
[36] *R v Secretary of State for the Home Department, ex p Brind* [1991] 1 AC 696 para 757 – 8.

debated in both Houses of Parliament and subsequently approved and deemed to be "consistent with advice received from senior members of the services."[37] The four individuals brought actions for judicial review claiming the decision to discharge was irrational and contrary to Article 8 ECHR. Citing *National and Local Government Officers' Association,*[38] which in turn cited *Brind*, the High Court rejected the application. The individuals appealed but this too was dismissed. It was found that because the policy had been so widely approved in Parliament, and consequently found to be consistent with advice received, the policy could not be deemed unreasonable.[39]

It should be noted that when the individuals appealed to the ECtHR in *Smith and Grady v UK*, the ECtHR criticised the strict application of *Wednesbury*. Stating that the threshold at which the High Court and Court of Appeal could find the Minister's decision to be irrational was "so high that it effectively excluded any consideration by the domestic courts of the question of whether the interference … answered a pressing social need or was proportionate to the national security and public order aims pursued."[40] It is from here that the concerns about the limitation of the JCs to judicial review principles stems. That if the JCs were to apply the *Wednesbury* test to the Home Secretary's decision to authorise the warrant there would be very few instances where they could hold said decision to be unreasonable. The discretion of the Home Secretary to issue warrants is the result of legislation which was much debated in Parliament. If the JC's performed their functions to this standard there would only be the illusion of oversight, it would only apply a thin veneer of legality to the Secretary's actions. However, it is not clear that this is the standard the JCs will apply in practice.

Moreover, it is not clear that proportionality will lead to a higher standard of review, given that the JCs are limited to principles of judicial review and as such are restricted to reviewing the decision-making process of the Secretary of State. As both proportionality and *Wednesbury* involve the same kind of reasoning, specifically consideration of weight and balance. As noted in *Pham*, these tests can lead to the same outcome.[41] The Supreme Court in *Pham* held that relative weight can and is assessed under *Wednesbury*, and that proportionality and *Wednesbury* may be very similar in practice. Lord Sumption observed that where *Wednesbury* review takes a high scrutiny approach, it can be described as

[37] *R v Ministry of Defence, ex p Smith* [1996] QB 517, para 517.
[38] *National and Local Government Officers' Association* (1992) 5 Admin LR 785.
[39] John Stanton and Craig Prescott, Public Law (2edn OUP 2020) p 496.
[40] *Smith and Grady v UK* (1999) 29 EHRR 493.
[41] *Pham v Secretary of State for the Home Department* [2015] UKSC 19, [2015] 1 W.L.R. 1591 para 60.

"proportionality at common law."[42]Within certain contexts then, such as national security, it is unclear that there is much difference between proportionality and *Wednesbury*.

Second, it is useful to set out exactly what is meant by proportionality in this context. While there are many formulations of the proportionality test, the one which is discussed here is as follows:

1. Does the measure impinge upon a highly-regarded interest (eg a human right)?
2. Does the measure pursue a legitimate objective?
3. Is the measure capable of securing that objective?
4. Is the adoption of the measure necessary in order to secure that objective?
5. Are the losses inflicted by the measure justified, or outweighed by the gains which it purchases(so-called narrow proportionality?[43]

One of the benefits of this formulation is that while one of the much-vaunted benefits of the proportionality test is the greater potential for analytical clarity when compared to *Wednesbury*, this potential can only be realised if courts are clear about what elements the test comprises and the role played by each.[44] Thus distinguishing clearly between stages 4 and 5 is essential. The fact that a right has been restricted to the minimum extent necessary to secure a particular objective does not mean that limitation is proportionate to the good that will flow from securing the relevant objective.[45] This distinction is particularly important to this discussion as it is likely part of a JC's evaluation process when reviewing a warrant application, given the national security context of the IPC.

While this is a technically correct formulation of the proportionality test it remains unclear which formulation of the test the UK courts apply. The IPCO advisory note, referenced above, states that the JCs will use a proportionality test but this does not make clear which formulation of the test is to be used. The leading formulation as set out in *De Freitas*[46] and adopted by the House of Lords in *Daly*,[47] does not unambiguously incorporate stage 5 of the

[42] Ibid paras 107 – 109.
[43] Mark Elliot, 'Proportionality and Deference: The Importance of a Structured Approach' (2013) University of Cambridge Faculty of Law Research Paper No. 32/2013, Available at SSRN: https://ssrn.com/abstract=2326987 or http://dx.doi.org/10.2139/ssrn.2326987
[44] Ibid p.2.
[45] Ibid.
[46] *De Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing* [1999] 1 AC 69, para 80.
[47] *R (Daly) v Secretary of State for the Home Department* [2001] 2 AC 532.

above test, narrow proportionality.[48] Where narrow proportionality is acknowledged as a requirement of the proportionality test it remains deeply ambiguous.[49] In some instances narrow proportionality is included as a fifth stage of the English doctrine of proportionality, clear and distinct from the necessity question. In other instances it is formulated as the "striking of a fair balance between the rights of the individual and the interests of the community",[50] and is characterised as being synonymous with proportionality,[51] so that the single question of fair balance can supplant the other questions outlined above.[52] The ECtHR on the other hand has used fair balance to refer to a requirement which replaces questions 4 and 5, effectively fusing necessity and narrow proportionality.[53]

There is further ambiguity with question 4, on necessity. In certain contexts, it is taken to mean that a measure may not be lawfully adopted unless it imposes the minimum restrictions on the relevant right which are consistent with achieving the legitimate objective.[54] In other circumstances it is characterised in less exacting terms, for example, in the ECtHR's standard formulation of necessity where an interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.[55] This suggests that the necessity question has no independent meaning, only deriving its meaning from questions 2 and 5.[56] The ambiguous nature of the proportionality test makes it difficult to see whether the proportionality test applied by the JCs will necessarily lead to a higher standard of review.

The Supreme Court, for example, does not consider the difference between *Wesdnesbury* and Proportionality to be stark, as the reasoning involved in the former can be similar to that in the latter. In *Kennedy v Information Commissioner*, Lord Mance held that "the common law no longer insists on the uniform application of the rigid test of irrationality once thought applicable under the so-called Wednesbury principle … the nature of judicial review in every case depends on the context."[57] This was cited in *Pham* by Lord Carnwath as an example of where a majority of the Supreme Court endorsed "a flexible approach to principles of judicial

[48] Mark Elliott, 'Proportionality and Deference: The Importance of a Structured Approach' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2326987> accessed 1 February 2021 p2.
[49] Ibid.
[50] *R (Razgar) v Secretary of State for the Home Department* [2004] 2 AC 368 para 20.
[51] *Kay v Lambeth London Borough Council* [2006] 2 AC 465.
[52] *R (Baiai and another) v Secretary of State for the Home Department (Nos 1 and 2)* [2008] QB 143 para 37.
[53] *James v UK* (1986) 8 EHRR 123 para 51.
[54] *A v Secretary of State for the Home Department* [2005] 2 AC 68 para 231.
[55] *Olsson v Sweden* (1989) 11 EHRR 259 para 67.
[56] Mark Elliott, 'Proportionality and Deference: The Importance of a Structured Approach' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2326987> accessed 1 February 2021 p3.
[57] *Kennedy v Information Commissioner* (2014) 2 WLR 808 paras 51 – 55.

review, particularly where important rights are at stake."[58] Lord Reed added to this, citing cases in which Parliament authorised significant interferences with important rights.[59] In such cases the court interpreted statutory powers that interfered with those rights as being subject to implied limitations, and adapted an approach amounting in substance to a requirement of proportionality, although less formally structured than under the HRA.[60]

While the difference between the two in practice is not great, it remains indeterminate whether the JCs will apply a *Wednesbury* standard of review or a proportionality standard of review, While the Act itself clearly states that in reviewing these conclusions the Judicial Commissioner will apply the same principles as would apply on an application for judicial review,[61] it is less clear what this means in practice. The JC must review the conclusions with a sufficient degree of care to ensure that they comply with the duties imposed by section 2 of the IPA 2016 (general duties in relation to privacy). If the Judicial Commissioner refuses to approve the decision to issue a warrant the Secretary of State may either (a) accept the decision and therefore not issue the warrant or (b) refer the matter to the Investigatory Powers Commissioner for a decision, effectively bypassing the Judicial Commissioner.[62] The option of the Secretary to effectively bypass the JC if they are not satisfied with their decision will be considered below.

The Act stipulates that the Commissioner will be limited to judicial review principles while also reviewing the conclusions to ensure compliance with the general duties in relation to privacy derived from the HRA. It remains unclear what form of judicial review will be applied in practice by the JCs. The limitation to judicial review principles implies a limitation to Wednesbury rationality review, while the reference to section 2 of the IPA implies considerations of the requirements of the HRA, and thus a proportionality review. This echoes Kavanagh's comment on the *Belmarsh* case above, that the court will apply a variable intensity standard of review based on the context of the case before it. However, in the first IPCO Advisory note, the Investigatory Powers Commissioner notes that the purpose of the so-called double-lock provisions of the Act are to provide an independent judicial safeguard as to the legality of warrants, in particular their necessity and proportionality. The Judicial

[58] *Pham v Secretary of State for the Home Department* [2015] UKSC 19 para 60.
[59] *R v Secretary of State for the Home Department, Ex p Leech* [1994] QB 198, *R (Daly) v Secretary of State for the Home Department* [2001] 2 AC 532.
[60] *Pham v Secretary of State for the Home Department* [2015] UKSC 19 para 118.
[61] IPA 2016 s 4.14.
[62] Ibid s 4.16.

Commissioners "will not therefore approach their task by asking whether a Secretary of State's decision that a warrant is necessary and proportionate is *Wednesbury* reasonable, as this would not provide the requisite independent safeguard."[63] So, then, while the legislation does not state the standard of review clearly, the IPC itself considers proportionality to be the appropriate standard of review. Nonetheless, this section will show that this distinction between *Wednesbury* and proportionality is ineffectual in the JC context as they are limited first and foremost to the test set out in the legislation.

In the drafting stage of the IPA, this question of standard of review proved a contentious issue. The Bingham Centre argued that the Act effectively limited the JCs to a *Wednesbury* standard of review. It stated that, while the questions of the necessity and proportionality of the warrant would be considered more where the HRA was engaged, the likely standard of review applied would result in authorisation in the absence of a finding of irrationality.[64] Hickman disagreed, stating that the fact that the JCs will be mandated to apply judicial review principles does not mean they will apply a *Wednesbury* review - "It is trite law that in human rights cases courts will decide for themselves whether a measure is necessary and proportionate and these are the judicial review principles that judges will surely adopt".[65]

There is some merit in these concerns as to the standard of review to be applied in a national security context. The Justices in *Carlile* disagreed about the standard of review applicable to the Home Secretary's decision in balancing UK foreign policy against the Article 10 ECHR rights of an individual. Lords Neuberger and Clarke, and Lady Hale agreed that proportionality was in principle the applicable standard of review. Lord Sumption disagreed, stating that the fact that Article 10 ECHR enshrines a core right of the Convention, does not cement proportionality in its fullest form as the applicable standard of review. In Lord Sumption's view some executive decisions were entitled to increased judicial respect because of their subject matter, and hence a lesser intensity of review. In particular he was referring to the national security context concerning assessments of risk. He concluded that "rationality is a minimum condition of proportionality but it is not the whole test. Nonetheless, there are cases where the rationality of the decision is the only criterion which is capable of judicial assessment".[66] He drew on *Corner House Research v Director of the Serious Fraud Office*[67]

[63] IPCO Advisory Note para 19.
[64] Bingham Centre for the Rule of Law – written evidence (IPB0055).
[65] Dr Tom Hickman – written evidence (IPB0039) para 5.
[66] Lord Sumption in *Carlile* para 32.
[67] R. *(Corner House Research and Another) v Director of the Serious Fraud Office* [2008] UKHL 60.

to show that, in the face of strong enough countervailing executive interests, no constitutional values - not even Convention rights or the rule of law - were immune from compromise.[68]

This framing of 'either *Wednesbury* or proportionality*'* is likely lacking in clarity within the context of national security. The issue is not stating '*Wednesbury* or proportionality' by rather using the word 'proportionality' – as it suggests a homogenous standard when in fact the standard varies in different contexts and even within particular contexts is fact-dependent. This brings into question the focus given to this framing in the submissions by the Bingham Centre and others highlighted above. It is sometimes presumed that proportionality is inherently more stringent a test than the *Wednesbury* rationality test but, as stated above by Lord Sumption, there are circumstances that can blunt the proportionality test to an evaluation of rationality. Then the court will apply the appropriate standard of review based on two key issues: the subject matter of the case and the level of deference afforded to the decision maker under review. Returning to the issue of deference in a moment, the importance of the subject matter is key to understanding the standard of review the JCs will likely apply. To put a finer point on it, the appropriate standard of review applied will depend on the context of the warrant application itself.

It is tempting to think that this form of substantive review[69] in the context of the double-lock system will likely result in a more stringent level of review. The argument for this would be that all bulk powers warrants engage at the very least Article 8 ECHR and can only be invoked in terms of being necessary for national security purposes. In light of this subject matter the JC will most likely adopt a correspondingly stringent review focusing on the necessity and proportionality of the measures set out by the warrant. This is due to how human rights review is different from non-human rights review in three key respects. First, a more intense form of proportionality is automatically involved in cases involving fundamental rights. Next, the process of decision making is relevant in human rights cases. If the decision-maker has struck a balance between the human right and the pursued legitimate objective themselves, this balance will be examined by the court. Conversely if the decision-maker has not even attempted to strike a balance the court is more likely to find the decision to be disproportionate. Finally, in human rights cases the government has the burden of proving in its defence that the rights-breaching decision was justified. Whether *Wednesbury*

[68] Hayley Hooper The future is foreign country (2015) 74 C.L.J 23-26.
[69] Rebecca Williams. 2017. "Structuring Substantive Review." (2017) 1 Public Law 99–123.

or proportionality is applied, these three distinctions remain in human rights review. They arise directly from the subject matter.[70] They feed into the contextual analysis made by the JC. It is this combined with the question of deference which determines how stringent the test applied by the JCs will be.

8.3 Judicial Commissioners - Discretion and Deference

An evaluation of the IPC as a fundamental safeguard for the ECtHR must therefore go beyond this false dichotomy of *Wednesbury* or proportionality. Given that the standard of review will be determined contextually based primarily on the subject matter of national security, the weight placed on deference owed to the executive by the JC increases. This section examines this issue doctrinally before the following section which examines extra-doctrinal factors which might impact the level of deference.

It is important to note that, when assessing the proportionality of the measures contained in a warrant, the task of the JC will not be to find the most proportionate measure the Secretary of State could authorise. Rather the task is to determine whether the Secretary's decision to authorise the measures in question was proportionate. There may be many more or less proportionate measures the Secretary could have accepted or advised the SIA to consider in their warrant application, but this is outside of the proportionality assessment conducted by the JC. In this instance the JC is not supplanting the Home Secretary's view on what should be done with their own, rather they are stopping the Home Secretary from authorising an unlawful act and leaving to their discretion which of the other more proportionate options to choose. Likewise, if the JC was to substitute the Secretary of State's view on how to proceed with the warrant, the executive's discretion would be severely limited. While this may seem to a preferable option for those seeking to maximise human rights protection, this would likely be considered judicial over-reach considering the judiciary's lack of institutional competence on matters of national security and lack of democratic accountability.

In light of the risk of judicial over-reach the courts have developed the concept of deference. To some this doctrine is purely contextual,[71] whereas to others it is tied to judicial expertise: a court must exercise restraint when reviewing the decisions of a person or body possessed

[70] ibid p 25.
[71] Murray Hunt, "Judicial Review after the Human Rights Act" [1999] 2 QMWLJ 14 15 – 16.

with specialised expertise.[72] It has been described as analogous, though not identical, to the ECtHR's doctrine of the margin of appreciation.[73] Some take a more critical view of the concept, arguing that when courts defer they are effectively refusing to determine whether the decision in question is lawful. In doing so they are guilty of dereliction of duty as judges.[74]

Applying this position to the present context, it would certainly be a dereliction of duty for the JCs to adopt a policy of complete deference to the decisions of the Secretary. However, this is not a policy which the JCs are likely to adopt. One reason for this is that the Judicial Commissioners are current or retired judges. Rather they are likely to adopt an approach similar to Lord Bingham's in *Belmarsh*, wherein they defer on the question of risk assessment but engage substantively on the necessity of the proposed measures. A position of deference which Allan himself agrees with. Just as framing which test should be applied as rationality (weak) versus proportionality (strong) is likely incorrect, so too is framing the level of deference owed to the executive as all or nothing.

Deference simply involves the court, where appropriate, attaching particular weight to the view of the decision-maker. This is tied into the wider concept of judicial restraint which "governs the extent to which, or the intensity with which, the courts are willing to scrutinize a legislative decision and justification advanced in support of that decision".[75] While Kavanagh discusses judicial restraint in the context of constitutional review, several of her clarifications of what judicial review means can be applied to understanding the likely approach of the JCs here.

First, judicial restraint is a matter of degree. It is not a matter of absolutes where the judges never interfere with legislative decision or never review legislation in a probing and robust way. Rather it is the principle that judges should exercise a degree of restraint in appropriate circumstances.[76] Likewise the likely approach of the JCs is not going to be one where they rubber stamp every warrant placed before them, but there may be circumstances in which a JC will need to exercise restraint and show some deference to the judgment of the Home

[72] David Pannick, "Principles of Interpretation of Convention Rights under the Human Rights Act and the Discretionary Area of Judgment" [1998] 98 Public Law 545 – 551.
[73] Edwards, Richard A. "Judicial Deference under the Human Rights Act." *The Modern Law Review* 65, no. 6 (2002): 859-882.
[74] T.R.S. Allan, "Human Rights and Judicial Review: A Critique of "Due Deference"" (2006) CLJ 685, 686
[75] Aileen Kavanagh, 'Judicial Restraint in the Pursuit of Justice' (2010) 60 University of Toronto Law Journal 23. p 25.
[76] ibid p 27.

Secretary. Given that every JC is either a current or retired senior judge, it appears unlikely that they would rubber stamp each warrant approval placed before them. Second, judicial restraint is a matter of self-restraint. In the constitutional review context this refers to the fact that it is for the courts to define the limits of their role in constitutional adjudication and determine the constitutionally appropriate degree of restraint.[77] In the double-lock context it is for the JCs to interpret what is the appropriate level of scrutiny they should bring to bear on the warrants brought before them. Although, as set out above, the JCs are limited to the test set out in the statute which limits this discretion. The JCs will decide the appropriate level of restraint, or deference, to show to the executive based on the subject matter before them, in accordance with the power vested in them by the legislation.

Third, when the courts decide that legislation infringes human rights at the constitutional level, they effectively place limits on the powers of the legislature to enact whatever legislation it wishes. The more willing the courts are to find legislation to be in breach of these rights, the greater the limit it places on the legislature. This has a lesser effect in the double-lock context, but whenever a JC rejects the decision of the Secretary of State to approve a warrant, they are effectively enforcing the boundaries of the Home Secretary's power. Fourth, the exercise of judicial restraint should not be equated with passivity or doing nothing. This clarification is harder to relate back to the present context but considering the power of the Secretary of State to appeal the decision of an individual JC to the IPC it may be in the interest of the JC to effect some level of restraint, or deference, in regard to some aspect of the warrant's proposed measures, such as the duration of the warrant. This restraint may cause the Secretary of State to more readily accept restrictions on another part of the warrant, such as the operational purposes.[78] This is a reputational argument for restraint as it puts forward that the JCs should take a restrained approach to decision making in order to protect and enhance their own reputation.[79] This approach was extra-judicially endorsed by the British judiciary when the HRA was being implemented. Lord Woolf for example noted that the objective of such an approach "should be to convince the legislature and the executive that the supervision of the courts is wholly constructive."[80] Likewise the JCs may

[77] Ibid p 28.
[78] Ibid.
[79] Ibid p 35.
[80] Lord Woolf, 'Current Challenges in Judging' (Paper presented to the Fifth Worldwide Common Law Judiciary Conference, Sydney, Australia, 10 April 2003) online: Judiciary of England and Wales < http:// www.judiciary.gov.uk/ publications_media/speeches/ pre_2004/lcj 1 00403.html>.

take a restrained approach in order to improve and protect their reputation with the Home Secretary, such that the executive is more willing to accept the restrictions mentioned above.

In practice deference is invoked in relation to two questions; necessity and proportionality.[81] Returning to question 4 outlined above on necessity , it may be appropriate to defer on the question of whether it is necessary to compromise a human right in pursuit of conflicting legitimate aim. This is a question of institutional competence, is the court in a position to form its own view on this point or should it either take the Government's word at face value or should it simply attach considerable weight to the Government's view on this matter. In the *Belmarsh* case for example, the Court did not need specialised expertise in order to decide the executive's action was not necessary. The Government had been detaining suspected foreign terrorists without charge or trial for national security purposes. Given that they had not detained UK nationals who were suspected terrorists, Baroness Hale held that "if it is not necessary to lock up the nationals it cannot be necessary to lock up the foreigners."[82] No special knowledge or expertise was needed to know this. However, it should be noted that in the preceding *Belmarsh* case, in the Court of Appeal, the Court used a different control group to the House of Lords and found in favour of the Secretary of State,[83] showing that this too is indicative of the courts taking a contextual approach rather than a settled doctrine. To draw this back to Judicial Commissioners, if the Home Secretary approved a warrant which authorised bulk interception in response to the threat posed by an individual British citizen, the JC would not need any experience or specialist knowledge to know that this was a disproportionate measure and reject the warrant. Bulk interception is only permittable if it is foreign focused. So then while there may be instances where the JCs can rule on necessity, it cannot be assumed that they will always be able to rule on necessity. It will come down to the specific question the JC is asked to review.

As a comparison, consider *Nicklinson,* a case concerning the ban on assisted suicide and its impact on the right to respect for private life.[84] The specific question before the court was whether said ban was a proportionate restriction on the right. This gave rise to another question as to whether the ban was a necessary means of protecting vulnerable people who may, in the absence of said ban, feel pressured into availing themselves of assisted suicide.

[81] Mark Elliott, 'Proportionality and Deference: The Importance of a Structured Approach' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2326987> accessed 1 February 2021. P4.
[82] *A v Secretary of State for the Home Department* [2004] UKHL 56 para 231.
[83] *A v Secretary of State for the Home Department* [2004] Q.B. 335 para 102.
[84] *R (Nicklinson) v Ministry of Justice* [2014] UKSC 38, [2015] AC 657.

The majority of the court were not prepared to rule that this ban was unnecessary, rather they opted to recognise the institutional competence of the decision-maker in this regard. Lord Sumption in particular noted that Parliament was better able to resolve "the controversial and complex questions of fact arising out of moral and social dilemmas" like those raised here as it has "access to a fuller range of expert judgment and experience than forensic litigation can possibly provide".[85] While this was directed at Parliament the same logic can be extended to the Government as well. In the JC context this would be similar to the JC being asked to consider the Secretary of State's approval of a targeted equipment interference of a vulnerable person's computer in response to a possible terrorist threat from that individual. While it would be within the JC's reach to insist on stricter safeguards corresponding to the individual's vulnerable status, the initial decision to consider such an infringement of the individual's rights necessary remains within the Secretary of State's discretion.

Another ground on which the Courts may defer to the decision-maker's view when addressing proportionality in the strict sense is the question of whether there is an adequate relationship of proportionality between the restriction on the right and the positive obligations flowing from the restriction.[86] A key source to draw on in elucidating this point is the *Carlile* case, specifically the contrasting majority and minority of opinions of Lord Sumption and Lord Kerr respectively. The case dealt with the infringement by the Home Secretary of an individual's Article 10 rights based on the belief that allowing said individual into the UK to meet with parliamentarians would lead to a threat to UK national security and foreign policy. The question before the Supreme Court came down to the level of deference the Court owed to the executive when balancing convention rights against a predictive threat; specifically, whether the restriction of Article 10 could be justified by reference to the public interest of safeguarding UK foreign policy.

By a majority, the Court refused to hold the actions of the Secretary of State to be disproportionate. Lord Sumption appealed to the democratic accountability of the executive's decision as evidence that it should be respected. Even when fundamental rights are at stake; "there remain areas which although not immune from scrutiny require a qualified respect for the constitutional functions of decision-makers who are democratically accountable."[87] This

[85] Ibid para 232.
[86] Mark Elliott and Robert Thomas, *Public Law* (4th edn, OUP 2020) p 560.
[87] *R (on the application of Lord Carlile of Berriew QC and others) v Secretary of State for the Home Department* [2014] UKSC 60 para 28 (Sumption L).

was echoed by Baroness Hale who stated that the narrow proportionality question "involves weighing or balancing values which many may think cannot be weighed against one another."[88] By this Baroness Hale meant that the weight ascribed to the UK's foreign policy interests and freedom of expression comes down to a value judgment on which reasonable minds can and do differ.[89] The courts should be mindful in such matters that the government is accountable to Parliament in a way that judges are not. Thus, in such circumstances it is appropriate for the court to attribute weight to the government's assessment of where the balance should lie.

The judgments in *Carlile* are relevant to the current discussion of the appropriate role of the JC in double-lock system discussed here as it outlines the judiciary's positions on deference in a human rights and national security context. Like *Carlile*, in reviewing a decision to approve a warrant the JC is effectively reviewing the actions of the executive in imposing a restriction on a qualified human right for the sake of national security based on risk assessment. Foreign policy and national security would both traditionally regarded as matters for the executive. What deference is owed to the executive in such a case? Lord Sumption took the position that the constitutional role of the Court was dictated by both principle and pragmatism. Specifically, this referred to the influence of the constitutional principle of the separation of powers and the pragmatic constraints involved in the judicial scrutiny of an executive decision concerning sensitive and predictive issues, such as foreign policy and national security.[90] He then rejected the role of the doctrine of general deference on two grounds, the fact sensitive nature and content of decisions relating to foreign policy and national security. Regarding the former, Sumption held that the fact sensitive nature of these decisions prevents the creation of general principles of deference.[91] Regarding the latter, Lord Sumption ruled that cases concerning foreign policy and national security decisions of the executive were to be recognised as questions of 'judgment and policy' as opposed to questions of law.[92] To him, the HRA did not modify the constitutional judicial role: "The

[88] *R (on the application of Lord Carlile of Berriew QC and others) v Secretary of State for the Home Department* [2014] UKSC 60 para 104 (Hale L).
[89] Mark Elliot and Robert Thomas, *Public Law* (OUP 2014) p561.
[90] Hayley Hooper The future is foreign country (2015) 74 C.L.J 23-26.
[91] *R (on the application of Lord Carlile of Berriew QC and others) v Secretary of State for the Home Department* [2014] UKSC 60 para 22 (Sumption L).
[92] ibid para 23 (Sumption L).

Human Rights Act did not abrogate the constitutional distribution of powers between the organs of the state which the courts had recognised for many years before it was passed".[93]

Lord Sumption appears to take two positions in *Carlile* which when applied to the JC context are unsustainable. Lord Sumption's position on deference in *Carlile* appears to be that the judiciary should defer based on the facts presented to them. In other words, they should take a contextual approach to deference. Applying this position to the JCs results in a system where the JCs accord deference to the executive based on the facts of the warrant before them, rather than a set amount of deference due to the warrant concerning national security. This would line up with the previous discussion of JCs engaging substantively with the review rather than just following a Wednesbury or proportionality standard of review. At the same time Lord Sumption is seeking to abrogate the judiciary's role in deciding cases concerning foreign policy or national security and risk assessment. Foster describes this as a dual approach with respect to judicial review: one encompassing the greater level of interference allowed for by the HRA, and another that applies in cases affecting national security and public safety.[94] It is here where the application of Lord Sumption's position contradicts the purpose of the JCs as an effective safeguard. The application of this position in the JC context would result in the JCs acting as rubber stamps to the actions of the executive and thus disqualify their efficacy as a safeguard.

In complete contrast to Sumption, Lord Kerr took the position that if the system is functioning properly it is for the courts to have the final word where Convention rights are at stake.[95] Although the Court should recognise the Home Secretary's "special institutional competence" in foreign policy and national security, there was no such competence when it comes to assessing the importance attached to human rights.[96] While this was the minority opinion in this case it did garner sympathy from the majority.[97] Lord Neuberger held that "the Court cannot simply frank the decision, but it must give the decision appropriate weight, and that weight may be decisive."[98] Hooper argues that this recognition that the HRA

[93] Ibid para 28.
[94] Steve Foster 'Stop me if you've heard this one before: judicial deference in free speech and security cases', Cov. L. J. 2015, 20(1), 58 – 67.
[95] *R (on the application of Lord Carlile of Berriew QC and others) v Secretary of State for the Home Department* [2014] UKSC 60 para 150 (Kerr L).
[96] Ibid para 155.
[97] Ibid para 105 (Hale L), ibid para 115 (Clarke L).
[98] Ibid para 68 (Neuberger L).

constitutionally modifies the role of the Court is to be welcomed, as it definitively authorises an independent evaluation of the balance between policy aims and Convention rights.[99]

However, applying Lord Kerr's position to the double-lock context may result in a problematic situation wherein the discretion of the Secretary of State is severely limited. In theory the JC always giving the actions of the Secretary of State the highest degree of scrutiny would result in a greater level of human rights protection. In practice the JC may exercise restraint for the reasons outlined above. The judiciary still lacks the specific institutional competence the executive has in this context. Additionally, while the executive is less democratically accountable in practice than in theory it is still far more accountable than the judiciary.[100] Lord Neuberger's position, of not franking the decision but giving the decision appropriate weight, is more in line with traditional notions of deference but allows room for the JCs to substantively engage with the particulars of the approved warrant before them. The level of deference JCs owe the Secretary of State in reviewing their approved warrants is one which acknowledges the relative institutional competence and democratic accountability of the executive when compared to the judiciary. Specifically, the courts are willing to defer on the necessity portion of the proportionality test on the basis of relative institutional competence, and willing to defer on the balancing portion of the proportionality test on the basis of democratic accountability.[101] In the double-lock context this will always be concerned with balancing predicted threats to national security and the restrictions to human rights stemming from surveillance measures.

8.4 Judicial Commissioners – Structural and Institutional Factors

The JCs' approach is likely to come down to the specific context surrounding an individual warrant and the questions they are asked to review. Likewise, focusing on whether the JCs will conduct a *Wednesbury* rationality review or a proportionality review obfuscates more salient issues of how the JCs operate. Any sufficient evaluation of the JC's effectiveness as a safeguard will not depend on doctrinal analysis of how the JCs are likely to reason. A more lucrative vein may be to highlight surrounding structural and institutional factors on how they operate in practice, the use of any discretionary power is influenced by a number of factors including extra-legal ones. Any use of discretionary power is going to be influenced by

[99] Hayley Hooper The future is foreign country (2015) 74 C.L.J 23-26.
[100] Mark Elliot and Robert Thomas, *Public Law* (OUP 2014)p 399.
[101] Mark Elliott, 'Proportionality and Deference: The Importance of a Structured Approach' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2326987> accessed 1 February 2021. P5.

surrounding institutional factors. The decision field marks out the boundaries of the legal decision maker's mandate, creating the particular setting within which decisions are made. The field is defined by the law, the legal institution, and the legal bureaucracy in its formulations of policy.[102]

There are a number of factors which impact the JC's decision field. Such as the fact that the IPC is responsible for both the authorisation of warrants and the reporting of errors stemming from these authorisations discussed below. Another of these factors is the lack of *inter partes* argument. JCs will not hear representations by those adversely affected by the authorisation of the warrant. This is a key difference between the IPA and TPIMs/control orders. The absence of an adversarial challenge, or even a Special Advocate, means that the JC in question will have to both identify the arguments that might be advanced by those affected and then pass judgment on those arguments. Given this adversarial deficit, there is a danger that the JC will miss something which may have been put forward by the proposed subject(s) of the warrant, or even by a Special Advocate for the proposed subject(s). It seems logical to assume that in the absence of an opposing voice, the question of what to consider when deciding the warrant will be excessively influenced by the executive. As part of the Bowman report, on the Review of the Crown Office List, the *ex parte* nature of the permission stage of granting a claim for judicial review was changed to an *inter partes* procedure. This changed it from what Lord Diplock described as summary in nature,[103] to a procedure which is equivalent to the *inter partes* procedure found in ordinary civil litigation.[104] While the reform was aimed at increasing the efficiency of the judicial review procedures, the move to *inter partes* led to a higher degree of scrutiny of judicial review applications.[105] Thus, the JC should adopt a correspondingly stringent standard of review when reviewing the Home Secretary's argument for approving the warrant.

There is also the consideration that the proposed subject of the warrant, whose human rights will be infringed, will have no means of participation in this process. This issue could be alleviated to an extent by the involvement of a Special Advocate in the process, as was

[102] Keith Hawkins, *Law as Last Resort: Prosecution Decision-Making in a Regulatory Agency* (OUP 2003) p144.
[103] *R. v. Inland Revenue Commissioners, ex p. National Federation of Self-employed and Small Businesses Ltd* [1982] A.C. 617 para 644.
[104] Cornford, T and Sunkin, M 'The Bowman Report, Access and the Recent Reforms of the Judicial Review Procedure' [2001] PL 11.
[105] It should be noted that claimants following the Bowman reforms were increasingly unsuccessful in obtaining permission for Judicial Review, indicating that the *inter partes* procedure may have caused more strict judicial scrutiny. Bondy, V and Sunkin, M 'Accessing Judicial Review' [2008] PL 647.

instituted by the Swedish legislation for signals intelligence. In the Swedish system the Foreign Intelligence Court which approved warrants had an advocate present who argued from the perspective of the protection of human rights, both of the immediate subjects of a warrant and in general.[106] To the ECtHR the presence of this advocate, who could not appeal a decision made by the Foreign Intelligence Court or report any irregularities to supervisory bodies, compensated to an extent for the total lack of transparency in the court's proceedings.[107] This lack of *inter partes* argument, and its effect on the level of judicial scrutiny employed by the JCs, is a key issue for ECHR compatibility regardless of the standard of review. It too points towards the need for the JCs to engage substantively with the context of the warrants before them and conduct a stringent standard of review.

Another factor is the power of the Secretary to appeal the decision of a JC to the IPC. Under section 35(5), "where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a person's decision to issue a warrant under this Chapter, the person may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant."[108] This is not clarified further in the Code of Practice. The only restriction is that an urgent warrant which is refused may not be appealed to the IPC. Should the IPC reject the appeal there is no further avenue of appeal for the executive. Notwithstanding this, the fact that the Home Secretary has an automatic right of appeal on the basis that they did not receive their desired outcome weakens the efficacy of the JC's oversight. As reported thus far this power of appeal has only been utilised once, in 2017.[109] This automatic right of appeal is likely to present an issue with the IPA's compatibility under Article 8 ECHR, as will be demonstrated in the final chapter evaluation of this legislative regime.

8.4.1 Institutional Independence

Leaving the immediate context of how the JCs decide on the approval of warrants, there are institutional factors which play an important role in determining the efficacy of the safeguard provided by the IPC. These centre around the notion of perceived institutional independence. Under the IPA the Judicial Commissioner's Office is charged with both authorising warrants,

[106] Centrum fur Rattvisa v Sweden (2019) 68 EHRR 2 para 22.
[107] Ibid para 137.
[108] IPA s23(5).
[109] IPCO Report 2018 para 2.9, The most recent IPCO report (2020) covering 2019 states that the appeal function was not used in that year.

in the so-called double-lock system, and reviewing the operation of the investigatory powers by the SIAs. This is another controversial point of the Act. While many consider the merger of the functions of the multiple commissioners which existed under the RIPA into one entity to be beneficial,[110] others point out that combining these two functions into one body presents an issue for judicial function and public confidence.[111]

This issue arises from the current organisation of the IPC, which places these two different functions under one roof. Post-hoc investigations and monitoring of SIAs often involves interacting, and likely building relationships with the subject of the review. An important part of the judicial function and public confidence in said function is that persons exercising judicial function do not receive briefings from and do not meet formally or informally with those who may come before them.[112] Of potential relevance here is the maxim that no one should be the judge in their own case, or rather that no member of the judiciary should sit in a case in which their own interests would create the appearance of bias.[113] As demonstrated in the *Pinochet* case, the matter at issue wasn't whether Lord Hoffman was actually biased against the defendant, but whether certain circumstances made it appear that he might be biased.[114] While the IPC would not technically be deciding cases, its roles of overseeing the approval of warrants and reviewing the use of said warrants creates (at least the appearance of) a conflict of interest. Thus, there is a need for either an institutional or sub-institutional separation between the JCs who consider warrant applications and those who conduct investigations.

One way of achieving this would be to separate the Investigatory Powers Commissioner from the other Judicial Commissioners. Under the Act the Commissioner is a Judicial Commissioner in addition to his other roles. Without separation, the Commissioner is likely to have to investigate the consequences of his or her own decisions. How can the Commissioner meet the obligation to keep the operation of bulk powers under review without first reviewing his own decision to authorise the warrant?[115] This would seem to provide a

[110] BT – supplementary written evidence (IPB01151) para 8, London Internet Exchange (LINX) – written evidence (IPB0097) para 23(a), McEvedys Solicitors & Attorneys Ltd – written evidence (IPB0138) para 8.1
[111] Amberhawk Training Limited – written evidence (IPB0015) para 15, Dr Tom Hickman – written evidence (IPB0039) paras 77 – 79, Justice – written evidence (IPB0148) para 62.
[112]Dr Tom Hickman – written evidence (IPB0039) paras 77 – 79.
[113] Dimes v. Proprietors of Grand Junction Canal (1852) 3 H.L. Cas. 759 para 793.
[114] *R v Bow Street Metropolitan Stipendiary Magistrate, ex parte Pinochet Ugarte (No. 2)* [2000] 1 AC 119, House of Lords para 132.
[115] Amberhawk Training Limited – written evidence (IPB0015) para 15.

clear conflict of interest for the IPC. It impedes the ability of the IPC to provide the accountability which is required of oversight bodies and good governance generally.[116] Amnesty International likened this situation to investigations concerning allegations of Article 3 abuse in Iraq carried out by the UK military.[117] The UK High Court there referred to the problem highlighted by the ECtHR where investigating officers "formed part of the same hierarchy with no provision for institutional or individual independence".[118]

This issue of the perceived independence, or lack thereof, of the JCs continues to resurface in arguments about the IPA. The Bar Council holds that the cultural independence of the JCs can be retained in those Commissioners who are appointed from the High Court or above but they have some reservations as to how said JCs are appointed.[119] Rather than being appointed by the Prime Minister from a pool of either current or retired senior judges, the Bar Council suggests that such appointments should be made by the Judicial Appointments Commission, in consultation with the Lord Chief Justice.[120] This position was widely supported during the consultation stage of the Bill. The predecessor to the IPC, the Interception of Communications Commissioner's Office (IOCCO) told the Joint Committee on Human Rights that appointment by the Prime Minister dilutes public confidence and independence.[121] The United Nations Special Rapporteurs on promotion and protection of the right to freedom of opinion and expression, on the rights to freedom of peaceful assembly and of association; and the situation of human rights defenders argued that it compromised the independence and impartiality of the JCs.[122] Lord Carlile QC emphasised the importance that the IPC does not become politicised, thus appointment should remain independent of Government.[123]

The then Home Secretary Theresa May rejected this suggestion that appointment by the Prime Minister would have any implications for the independence of JCs. This was on the grounds that the current commissioners, the Interception of Communications Commissioner (IOCCO) and other predecessors to the IPC, were Prime Ministerial appointees and "there is no suggestion that they have not been independent in the operation of the work they have

[116] House of Commons Public Administration Select Committee, Good Government (HC 97 2008–09).
[117] Amnesty International UK – supplementary written evidence (IPB0074) 33.
[118] R (Ali Zaki Mousa) No.2 [2013] EWHC 1412 (Admin), [2013] HRLR 13 at 111-112.
[119] Bar Council – supplementary written evidence (IPB0134).
[120] Ibid.
[121] Interception of Communications Commissioner's Office—written evidence (IPB0101).
[122] UN Special Rapporteurs – written evidence (IPB0102).
[123] Joint Committee on Draft Investigatory Powers Bill para 584.

done".[124] The Joint Committee on the Draft Investigatory Powers Bill took May's position in not thinking that prime ministerial appointment would have any impact on the independence of the IPC and JCs. But still the Joint Committee recommended that the Lord Chief Justice should have the power to appoint JCs following consultation with his judicial counterparts in Scotland and Northern Ireland, the Prime Minister, Scottish Ministers and the First Minister and Deputy First Minister in Northern Ireland.[125] The Judicial Appointment Commission must also be consulted to ensure that the appointments procedure is fair and transparent. A modified version of this was included in the final IPA. The power to appoint remained Prime Ministerial but an individual could only be appointed if recommended jointly by the Lord Chancellor, Lord Chief Justice of England and Wales, Lord President of the Court of Session, Lord Chief Justice of Northern Ireland and, in the case of JCs, the Investigatory Powers Commissioner.[126]

While this is undoubtably an improvement on the initial appointment scheme outlined in the draft bill, it is unclear if requiring these recommendations abrogates the issues caused by Prime Ministerial appointment. If the purpose of the JCs is to provide effective judicial oversight over the actions of the executive operating under the IPA, then it is unclear what justification there is for the power of appointment to remain in the hands of the executive. Following on from this point, there is the question of the conditions of the JCs' re-appointment. Their re-appointment is subject to the joint recommendations outlined above. They are subject to three-year renewable terms which are simultaneously precarious and potentially indefinite. This produces a double incentive for the JC to act in accordance with how the executive wishes as there is the potential for indefinite employment should they please the executive. At the same time there is the possibility of being let go at the end of the three-year term. The ECtHR has ruled that four-year renewable terms are 'questionable' in the context of appointment of military judges sitting as members of National Security courts.[127]

Scott describes the IPC as a hybrid institution in that it is not fully a judicial body or political body. He points out that the double-lock system involves the Commissioners in the prior approval of warrants for the first time.. He argues that their ability to successfully perform

[124] Ibid para 586.
[125] Ibid paras 587, 588.
[126] Ibid.
[127] Incal v Turkey (2000) 29 EHRR 449 para 74.

this role will be in large part a function of their ability to remain outside of the executive: "to not allow their involvement in the process of granting warrants to undermine their work in holding to account, at the macro level, the regime of investigatory powers and those with primary responsibility for its operation."[128] This points to the need to separate the IPC's warrant approval function from its general oversight function.

In a similar vein, Woods et al argue that the JCs are effectively exercising an oversight function from within the executive, as opposed to from the judiciary. In making this claim they draw on several points which have already been explored in this chapter including the lack of inter partes argument, and that JCs must always have regard to national security as the prime consideration when reviewing warrant applications. The double-lock system under the IPA relies heavily on a clear separation of powers and an independent judiciary, yet "simultaneously risks compromising them."[129] While the Investigatory Powers Commissioner has stated that "Judicial Commissioners will act totally independently of government"[130], the IPA limits their powers of review and requires deference to ministerial judgment on national security decision making.[131] While the individual and institutional independence of JCs approaches what might be expected of the constitutional protections for the judiciary, the limits of oversight powers and the approval of executive actions (rather than judicial authorisation on application) seem to align more closely with oversight positioned within the executive. They compare this with the original recommendations of the Independent Reviewer of Terrorism Legislation[132], which were that in most instances the Secretary of State should apply for a warrant and a judge should decide whether to authorise it.[133]

Linking these factors to the ECHR, they may run afoul of some of the specific requirements of Article 6. Namely the objective element of Article 6 which places emphasis on structure or appearance when determining a party's doubts about a tribunal's independence and impartiality. In their case law the ECtHR has pointed to several relevant factors on this point.

---

[128] Paul Scott, (2019) Hybrid institutions in the national security constitution: the case of the Commissioners. Legal Studies, (doi:10.1017/lst.2018.44). p 27.
[129] Lorna Woods, Lawrence McNamara, and Judith Townend. "Executive accountability and national security." (2020) 84 The Modern Law Review 3, 25
[130] IPCO Press release,18 October 2017 at https://www.ipco.org.uk/docs/JC%20Announcement% 2020171018.pdf
[131] Lorna Woods, Lawrence McNamara, and Judith Townend. "Executive accountability and national security." (2020) 84 The Modern Law Review 3, P 25
[132] Ibid p 24
[133] David Anderson QC, *A Question of Trust: Report of the Investigatory Powers* Review paras 14.47 – 14.57

The manner of appointment and duration of office of the adjudicators[134], the existence of guarantees against outside interference[135], and the appearance of independence.[136] This issue will be examined further from an ECHR perspective in a subsequent chapter. The factors discussed in this section all point to perceptual issues of independence and legitimacy for the JCs. The appointment process, term limits and organisational set-up wherein the IPC is responsible for reviewing and providing oversight of its own work all point to the appearance of bias in the work of the JCs. This is not to say that the JCs are inherently biased in their work, only that these factors introduce a perceived element of bias into their work which undermines their perceived independence and legitimacy in the eyes of the public.

8.5 How do JCs review warrants?

With these factors in mind, how do JCs conduct their review of the Secretary of State's decision to issue a warrant? To elucidate this, it is useful to examine the process to issue a bulk interception warrant step-by-step. As this chapter has shown this limitation to the principles of judicial review is, in practice, irrelevant. There is a fear stemming from this subsection that the JCs will be limited to a *Wednesbury* style rationality review through the prohibition of a supposedly more stringent proportionality review. However, this fear is misplaced as the Supreme Court does not consider the difference between *Wednesbury* and proportionality to be stark. It is then likely that the JCs will apply a contextual approach focused on the subject matter and the appropriate amount of deference they should show the executive.

It is tempting to think that such a contextual approach will automatically lead to a more stringent standard of review. The subject matter in a bulk interception warrant will always concern an interference with Article 8 ECHR for reasons of national security. They involve the most intrusive powers and therefore their use needs particularly careful oversight. However, this cuts both ways as issues such as national security could have such a profound effect on the nation that the judiciary should defer to the executive. So, the context can influence the standard of review but this depends on how you view the context.

This indeterminacy places a lot of weight on the question of appropriate deference from the JC to the Secretary of State. The level of deference the JCs owe the Home Secretary is based

[134] *Le Compte, van Leuven and de Meyere v Belgium* (1982) 4 EHRR 1, para 55
[135] *Piersack v Belgium* (1983) 5 EHRR 169, para 27
[136] *Delcourt v Belgium* (1979-80) 1 EHRR 355

on two questions: the relative institutional competence of the judiciary and the executive; and, the democratic accountability of the executive. The level of deference JCs owe the Secretary of State in reviewing their approved warrants is one which acknowledges the relative institutional competence and democratic accountability of the executive when compared to the judiciary. Specifically, the courts are willing to defer on the necessity portion of the proportionality test on the basis of relative institutional competence, and willing to defer on the balancing portion of the proportionality test on the basis of democratic accountability.[137] In light of the indeterminacy of how the JCs will operate, deference may be seen as simply another factor in the JCs' contextual approach.

The JCs' approach will then depend on what they are asked to review. Specifically, this contextual approach will depend on which decisions they are asked to review. Returning to the questions above, the Home Secretary has four conditions to fulfil in approving the warrant, two of which are subject to review by the JC: necessity and proportionality. An examination of what the warrant should include reveals a distinct set of questions the Secretary of State must approve the answers to in approving the warrant:

(1) On what statutory grounds is the warrant sought considered necessary?
(2) What is the context of the operation the warrant seeks to authorise?
(3) Who is the warrant seeking to subject to interception?
(4) What communications are to be intercepted?
(5) What telecommunications or postal operator hosts the communications?
(6) How feasible is the interception?
(7) Is the conduct authorised by the warrant necessary?
(8) Is the conduct authorised by the warrant proportionate to what is sought to be achieved?
(9) Is there any collateral intrusion and is this intrusion justified?
(10) Are the communications in question likely to be subject to legal privilege?
(11) Is the purpose of the warrant to intercept LPP?
(12) Is the purpose of the warrant to authorise the interception of confidential journalistic material?
(13) Is journalistic material likely to be intercepted by the authorised interception?

[137] Mark Elliott, 'Proportionality and Deference: The Importance of a Structured Approach' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2326987> accessed 1 February 2021. P5.

(14) Is the application urgent? How is this urgency justified?

(15) Are there assurances that all material obtained under the warrant will be kept for no longer than necessary and handled in accordance with safeguards?[138]

(16) Are each of the operational purposes specified on the warrant is a purpose for which selection is, or may be, necessary?[139]

The level of deference the JC should show the Secretary of State will depend on which question, or aspect of the warrant is under review. For example, question 6 on the feasibility of the interception is clearly outside of the JC's competence and unless the proposed operation is on the face of it clearly infeasible they will defer to the Secretary's judgment regarding it. This is similar to the likely approach with more technical questions like number 5. The JC is less likely to defer on the questions of necessity (1 and 7), although they are more likely to defer on question 1 as the executive can reasonably claim that the warrant is authorised on national security grounds.

Regarding the target of the interception, the JCs' willingness to defer will depend on who the target is and what the specified communications are likely to be. The JCs are likely to defer to the Home Secretary's judgment if the target is a known terrorist such as Jihadi John, but in warrants where the target is of a protected category – such as being a journalist or member of Parliament– they may be less willing to defer as there are additional safeguards in place for these targets. Likewise, with the questions concerning LPP and confidential journalistic material, the JC is likely to take a more stringent level of review owing to the protected nature of such communications.

Question 14 on urgency is an outlier as, if the Home Secretary believes the warrant to be urgent, they can bypass approval by the JC. By the time it is reviewed by the JC it will have already been authorised and be in operation, lessening the impact of the review. Like so many of these questions it is unclear from this abstract position whether a JC will defer on this question or not. On one hand as urgency effectively bypasses the JC safeguard it must be used exceedingly sparingly or else it risks abuse, so the JC may take a strict standard of review with the authorisation. Thus, reducing the executive's discretion to use urgent warrants. On the other hand, urgent warrants are necessary when dealing with an imminent threat to national security. Due to the JCs' lack of democratic accountability and institutional

[138] Interception of Communications Code of Practice para 5.29.
[139] Ibid para 6.28.

expertise they may be wary of discouraging the use of these warrants. Question 15 is also an outlier as it is a question which the Home Secretary must consider but it is not mentioned specifically as something the JCs must review. Arguably it should be subject to review in such a contextual approach as the presence of adequate and sufficient safeguards is a key part of the ECtHR's test for the compliance of surveillance regimes with Article 8, forming a part of the Court's necessity test in particular.

Question 16 concerns one of the few examination safeguards present in the IPA, the Secretary of State must consider that the each of the specified operational purposes is a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary.[140] As discussed in the previous section on examination safeguards, operational purposes are a safeguard which effectively act as a list of purposes for which bulk surveillance can be ordered.[141] These are narrower than statutory purposes such as national security and are more likely to describe activities such as establishing links between known subjects of interest and to search for traces of activities by individuals who are not fully known by the SIAs. The Secretary's decision as to the operational purposes on the warrant should be reviewed stringently by the JC as the Secretary controls the list of approved operational purposes, with the only oversight to this control being another member of the executive: the Foreign Secretary. The IPA allows for this review as the question for the JC is whether each of the specified operational purposes is "a purpose for which the examination of intercepted content or secondary data obtained under the warrant is or may be necessary".[142] However, as discussed throughout this chapter, this is limited to reviewing the Secretary of State's conclusions.

It should be noted that the master list of operational purposes is subject to parliamentary oversight through the Intelligence and Security Committee of Parliament. The Secretary of State must present the list at the end of each relevant three-month period.[143] It is also subject to review by the Prime Minister who must review the list at least once a year.[144] It is notable that one of the few examination safeguards present in the IPA is here reduced to simply one of 16 considerations for the JC to consider.

[140] IPA 2016 s 138 (1)(d)(i).
[141] IPA 2016 s 142.
[142] IPA 2016 s 140.
[143] IPA 2016 s 142 (8).
[144] IPA 2016 s 142 (10).

While analysis of this construction of what the JCs' contextual approach gives some insight into how the JCs *may* operate it cannot give a definitive answer. While the questions inform us of what level of deference they are likely to take, the ultimate answer to that question will be heavily influenced by the subject matter of the warrant to the point where it is indeterminate to outside observers how exactly the JCs will operate. In light of this a more fruitful way to evaluate the Judicial Commissioners as a safeguard is to interrogate institutional factors in how they use their discretion.

Additional factors which will affect how the JCs will operate in practice include the lack of inter partes conflict and the ability of the Home Secretary to appeal the decision of the JC. Regarding the former, this lack of adversarial reasoning will force the JC to both construct the argument of the intended subject of the warrant before evaluating both their argument and the argument of the Secretary. This is liable to influence the reasoning of the JC. The adoption of a special advocate such as the one utilised in the Swedish Signals Intelligence framework was suggested in order to remedy this issue. The ability for the Secretary to appeal the decision of the JC to the IPC purely on the basis that they received an unsatisfactory result is one which is liable to influence the JC's reasoning. First it may cause the JC to defer more to the Secretary on certain questions as they are liable to appeal if the JC takes too harsh a view on one of the provisions of the warrant, or the decision process the Home Secretary took in approving it.

This is tied to some of the surrounding institutional issues with the JCs. The fact that the JCs are appointed on three-year renewable terms by the Prime Minister intersects with the executive's ability to appeal. A JC may be wary of making an enemy of the executive through conducting thorough reviews if it is liable to result in their term not being renewed. This issue could be resolved if the appointment process for the JCs was placed in the hands of the judiciary. While the appointment of the IPC and JCs is subject to recommendation by the judicial heads of the UK, it remains unclear what benefit there is to it being a prime ministerial appointment. These issues feed into an overall issue with the perceived independence and legitimacy of the JCs. There are extra-legal factors which must also be considered when discussing the efficacy of the JCs as a safeguard. While it is unclear what the ceiling of the JC safeguard is, the floor is one wherein the review of the Secretary's decisions applies only a thin veneer of legality to the executive's actions. Owing to the opacity of the JC's decision-making procedure this is an issue of perception. In order for this

authorisation to be considered an adequate and effective safeguard, what is perceivable should give the appearance of non-biased independent check on executive action.

8.6 Conclusion

Returning to the overall question of this thesis, do the authorisation and examination mechanisms within the IPA meet the ECHR and CJEU minimum requirements, and do they adequately protect against the harms of bulk surveillance. The answer to the former is clear, the double-lock system of warrant authorisation meets the minimum requirements of both Courts. The ECHR approach, as discussed in chapter 4, is that bulk interception should be subject to independent authorisation at the outset. The double-lock itself is a response to the ruling in *Big Brother Watch* against the IPA's predecessor where the authorisation of bulk interception was not subject to ex ante independent authorisation. While there are issues with the actual level of independence the IPC has, discussed below, the double-lock on its face is a system wherein the executive is subject to authorisation by an independent body which is staffed by former members of the judiciary, this appears to meet both the minimum requirement as per *Big Brother Watch*, and the CJEU requirement of overview by an independent but not necessarily judicial body as per *Digital Rights Ireland*.

Next, in *Big Brother Watch* the GC ECtHR set out that the need for safeguards is highest at the selection for examination stage involving an analyst. However, the selection for examination safeguards within the IPA are very limited. Namely they are limited to operational purposes forms one of the questions that must be considered by the JC at the issuing of the warrant. These operational purposes are quite broad and are, in effect, a narrowing of the statutory aims of national security to more specific aims such as protecting against violent jihadist groups. As the Grand Chamber in *Big Brother Watch* found that independent supervision at the selection for examination stage was not required, instead warrant descriptors supervised at the authorisation stage were sufficient, provided that they are sufficiently narrow. While it is argued here that the operational purposes are not sufficiently narrow it isn't clear that the ECtHR would accept this argument as the Court did not set out what it meant by sufficiently narrow.

On the question of overall human rights protection, while there is an appropriate role for the judiciary in authorising warrants within the IPA regime, the level of human rights protection they provide is indeterminate from outside the system. Due to the covert nature of surveillance, it is impossible to know how much deference the JCs afford the executive on a

given warrant. This indeterminacy places additional pressure to reform the institutional and structural factors which might influence the deference of the JCs such as the lack of inter partes conflict, the ability of the executive to appeal from the JC to the IPC, and inappropriate role of the executive in appointing the IPC and JCs. Without these reforms it isn't clear whether the IPC and by extension the double-lock warrant authorisation system is capable of protecting against the harms of bulk surveillance.

9. Review and Oversight in the Investigatory Powers Regime

This chapter follows on from the previous one in evaluating the review mechanisms and oversight present in the IPA regime; namely the auditing and inspections conducted by the Investigatory Powers Commissioners Office (IPCO), the annual reporting done by the IPCO, and the Investigatory Powers Tribunal (IPT). The IPCO is a key aspect of the IPA regime, the previous chapter discusses the role of the IPC and the JCs in the warrant authorisation process, here the review and oversight function of the IPC is analysed. This chapter shows that while the auditing and reporting efforts of the IPCO is thorough, they are ultimately flawed in their effectiveness due to the problem of transparency in covert surveillance.

The IPT is the primary ex post safeguard for the IPA bulk surveillance regime. As noted in the overview of ex post safeguards in chapter 2, several issues have arisen in the 20 years since the establishment of the IPT. These issues resulted in the enactment of the Investigatory Powers Act 2016. Arguably the reforms introduced by this Act have been an improvement, such as the removal of the obligation to sit in secret and the removal of the ouster clause. Interestingly, the removal of the ouster clause has removed the ability of the IPT to claim to be the sole arbiter of its procedure. It is unclear how this interacts with their ability to set their own rules under RIPA, as the IPT used their position as sole arbiter in order to defy the rule that it had to hold cases in secret.

This chapter builds on that overview by building a sustained critique of the Tribunal from a procedural justice perspective. This perspective is argued to be a more valuable means of evaluation than a substantive justice perspective owing to the inherently covert nature of the material the Tribunal deals with. This chapter proceeds first by examining the reporting by the IPT as to their rulings in aggregate, finding that the IPT is unlikely to find in favour of applicants. Next, the chapter provides an overview of procedural justice in the context of Article 8 ECHR before comparing three illustrative cases from the IPT's jurisprudence, as the case law of the IPT is available, even though there is a lot of it which isn't published.[1] In light of the lack of procedural justice demonstrated in these cases the chapter then examines comparators for the IPT: Public Interest Immunity and Special Advocates. The chapter

[1] The Investigatory Powers Tribunal: Closed and Open Procedures: https://www.ipt-uk.com/content.asp?id=13.

finishes by drawing recommendations from these comparators as to how the IPT can be improved.

Throughout this chapter the main question of this thesis will be returned to. First whether these safeguards meet the requirements of European human rights law as exemplified by the ECHR and CJEU. Next, whether these safeguards protect against the harms of bulk surveillance as discussed in chapter 4.

9.1 Auditing and Inspection by the IPCO

The IPCO inspections of the use of investigatory powers are done with three objectives in mind: (a) to ensure that compliant authorisations have been given, (b) to ensure that legal requirements (such as necessity and proportionality) have been met, and (c) that standards of good practice are maintained. The IPCO emphasises that one size of inspection does not fit all, that the IPCO is flexible in their approach to inspection to ensure the demands they make on public authorities are proportionate but allow them the required access.

An inspection consists of a number of steps. The inspectors will visit the authority in question, review documentation and interview relevant staff members. Examples of relevant staff members include operational and policy teams. The inspectors scrutinise records of the authority's use of an investigatory power. This includes: (a) the application for its use, (b) the authorisation approving its use, (c) applications to renew the authorisation and extend its use, and (d) documents cancelling the use of the power. In addition to these fundamental documents, inspectors review a variety of supporting documents such as risk assessments for covert human intelligence sources, policy documents, training modules and governance structures. Inspectors may also review samples of material obtained through the use of covert powers. The inspection also aims to ensure that the retention and deletion of this material is carred out in accordance with the Codes of Practice.

Significantly, one of the inspectors is a Judicial Commissioner. The IPCO states that this has a dual benefit. First, it enhances the JC's awareness of the context of operations, which is relevant to their consideration of warrant applications. Second, it gives the Commissioners an opportunity to directly challenge aspects of policy and methodology at individual authorities.[2]

[2] IPCO, 'Carrying out an inspection' (ipco.org.uk) <//www.ipco.org.uk/what-we-do/inspections/carrying-out-an-inspection/> accessed 29/09/2023

When selecting casework to inspect, the IPCO takes a random sample but also material that is based on specific priority factors such as the likelihood of obtaining sensitive material, areas of concern raised previously by the authority in question, areas of heightened public interest, issues highlighted through reported errors, and issues or trends highlighted by a JC.[3] Inspectors have unrestricted access to all relevant documents. Each inspection is done to give the inspectors insight into the processes and activities of the public authorities in question, and all material reviewed during an inspection is chosen by the inspectors, not the inspected authority.[4]

The IPCO sets out that their aim is not to review a fixed statistically representative sample because each inspection should be a process of gaining insight into the methodologies used by, and the activities of, the individual authority. Rather they might focus their attention on the adequacy of staff training.[5] With the exception of smaller establishments that do not use their powers often, and particular issues of concern such as the use of juvenile covert human intelligence sources, the IPCO does not attempt to view all the authorisations in any particular area.

The IPCO provides some limited statistics on their inspections on their website. Unfortunately the images showing the breakdown of inspections categorised by organisation type for the years 2021 – 2023 are missing due to broken links. However, the 2020 image is intact and shows the breakdown of the 342 inspections conducted in that year:

[3] IPCO, 'Selecting material for inspection' (ipco.org.uk) https://www.ipco.org.uk/what-we-do/inspections/selecting-material-for-inspection/ accessed 29/09/2023.
[4] Ibid.
[5] Ibid.

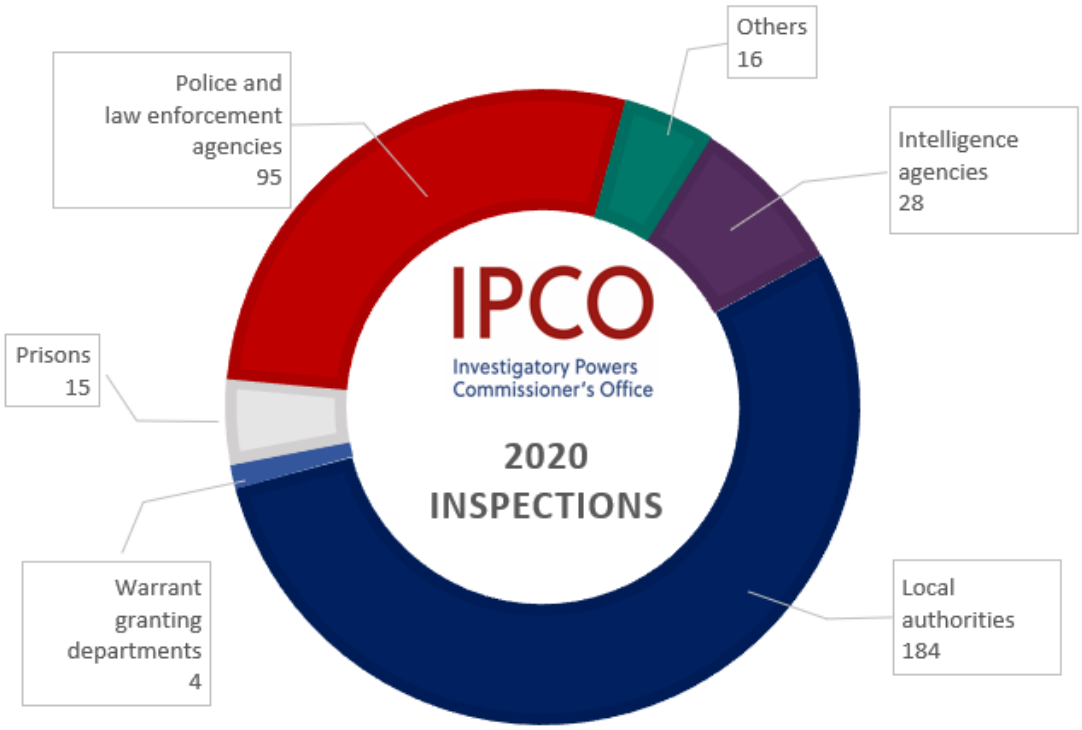

Figure 2. IPCO Audits and Inspections 2020

Local authorities and police and law enforcement take up the majority of conducted inspections, these authorities can only utilise targeted surveillance powers under the IPA. The intelligence agencies who can utilise bulk surveillance powers, such as GCHQ, consist of a minority of total inspections but considering the sheer number of police and law enforcement agencies and local authorities compared to the relatively few intelligence agencies, proportionally this appears to be adequate.[6]

9.1.1 Auditing Bulk Powers

The IPCO's auditing and inspection of the use of bulk powers has evolved since the implementation of the IPA. In 2018 inspections were conducted for the relevant powers twice a year at each agency. Prior to an inspection, the agency was required to provide a list of all the relevant authorisations and casework. This list included internal approval documents with sufficient detail for the inspection team to select additional material for further scrutiny.

[6] IPCO, 'Inspection Statistics' (ipco.org.uk) https://www.ipco.org.uk/what-we-do/inspections/inspection-statistics/ accessed 29/09/2023

In 2019 the IPCO performed their first full inspection of the equipment interference powers under the IPA at GCHQ. This inspection included retrospective oversight of internal processes to approve operations conducted under BEI warrants. To do this the IPCO selected cases in advance for scrutiny, discussing particular cases of interest with GCHQ's teams at the inspection. Next the IPCO gained direct access to IT systems used to request and approve bulk equipment interference warrants to select further cases for examination. Finally, the IPCO selected a variety of cases in order to ensure the examined cases were from a variety of business areas. Finally, as of 2020, the IPCO has added to its approach in order to reflect the ECtHR judgment in *Big Brother Watch*. The IPCO decided that their inspections would include a detailed examination of the search criteria used by the agencies. This was intended to supplement the oversight provided to bulk surveillance powers by the IPCO.[7]

9.2 Annual Review by the Investigatory Powers Commission Office

Another safeguard is the annual review of the use of Investigatory Powers conducted by the Investigatory Powers Commissioner. This is a general oversight mechanism. The IPC must, as soon as reasonably practicable after the end of each calendar year, make a report to the Prime Minister about the carrying out of the functions of the JCs.[8] As set out in the legislation these reports must include:

(j) statistics on the use of the investigatory powers which are subject to review by the IPC (including the number of warrants or authorisations issued, given, considered or approved during the year),
(k) information about the results of such use (including its impact),
(l) information about the operation of the safeguards conferred by this Act in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic information,
(m) information about the following kinds of warrants issued, considered or approved during the year –
    i. targeted interception warrants or targeted examination warrants of the kind referred to in section 17(2),

[7] IPCO, 'Carrying out an inspection - bulk powers' (ipco.org.uk) https://www.ipco.org.uk/what-we-do/inspections/carrying-out-an-inspection/bulk-powers/ accessed 29/09/2023.
[8] IPA s 234 (1).

ii. targeted equipment interference warrants relating to matters within paragraph (b), (c), (e), (f), (g) or (h) of section 101(1), and

iii. targeted examination warrants under Part 5 relating to matters within any of the paragraphs (b) to (e) of section 101(2),

(n) information about the operational purposes specified during the year in warrants issued under Part 6 or 7,

(o) the information on errors required by virtue of section 231(8),

(p) information about the work of the Technology Advisory Panel,

(q) information about the funding, staffing and other resources of the JCs, and

(r) details of public engagements undertaken by the JCs or their staff.[9]

Upon receipt of this report, the Prime Minister must publish it and present it to Parliament. Although the PM may, after consultation with the IPC, exclude any part of the report from publication if the PM thinks that such publication would be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the UK or the continued discharge of the functions of any public authority whose activities are subject to review by the IPC.

9.3 Meeting Human Rights Law Requirements

The specific requirement that applies to this annual review by the IPCO is the *Big Brother Watch* requirement that procedures for and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance are present. In the GC judgment of *Big Brother Watch* the ECtHR examined the predecessor to the IPCO, the Interception of Communications Commissioner. This predecessor in effect carried out the same oversight functions as the IPCO. The ECtHR highlighted that the IC Commissioner was independent of the executive and legislature, and had to have held high judicial office, with the principal duty to review the exercise and performance by the relevant authorities in their use of interception powers.[10] The Court also highlighted the IC Commissioner's 2016 report as providing evidence of the extent of his oversight powers.[11] Overall, The ECtHR held that the IC Commissioner provided independent and effective oversight of the regime.[12] The fact that he and his inspectors were able to assess the necessity

[9] IPA s 234 (2) (a-i).
[10] Big Brother Watch GC Para 407
[11] Ibid Para 408.
[12] Big Brother Watch GC para 425

and proportionality of a significant number of warrant applications as well as make recommendations to the heads of relevant public authorities were cited as evidence of this effective supervision.[13] Given that the IPCO is the direct successor to the IC Commissioner and, as detailed above, conducts the same functions as its predecessor it is likely that the ECtHR would the oversight provided by the IPCO to be similarly effective. However, this does not mean that oversight and review by the IPCO can effectively protect against the harms of bulk surveillance.

9.4 Protecting against the Harms of Bulk Surveillance: The Issue with Transparency

As indicated above, the IPCO reports as described in section 234 are very detailed and useful tools for promoting the transparency of the surveillance regime under the IPA. For example, they have already been used to show the JC's authorisation rates. However, the problem with this safeguard is that while they are transparent, transparency can only go so far in this field as a safeguard. It is inherently difficult to be transparent about a field which is by its nature covert. For example, the authorisation rates mentioned above present the simple binary of either authorised or not and offer little information on how the JC conducted their authorisations. Here, the publication of sensitive parts of the IPCO report can be censored by the PM following consultation with the IPC, an individual who owes their position to the PM. Beyond this there is seemingly a problem with these reports being full of detailed stats and figures which don't effectively communicate how these powers are being used or misused. O'Neill discusses this as the basic limitation of transparency: it ignores the necessary conditions for effective communication. "What is merely disseminated may not reach any, let alone relevant, audiences. Even if it reaches them, they may find the content disclosed unintelligible or impossible to assess."[14]

A good example of this is the reporting of errors by the IPCO. As per the IPCO 2017 report the IPCO carried out 33 error investigations into the misuse of surveillance powers. 24 of these were considered serious error investigations, of which 20 concerned human error while 4 concerned technical errors. Circumstances where an error can be classified as serious include: technical errors relating to CSP secure disclosure systems which result in a significant number of erroneous disclosures, errors where a public authority has acted on

[13] Ibid, para 412.
[14] Martin Moore "RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework" (2014) 85 The Political Quarterly 125

wrong data and initiated a course of action which has had an adverse impact on someone, and errors which result in the wrongful disclosure of a large amount of communications data or a particularly sensitive data set.[15]

The impacts of these errors can be wide-ranging and include the execution of a search warrant at the address of someone unconnected with an investigation or arresting unconnected individuals. These two impacts were present in 11 of the 24 serious error cases, with 19 people being affected. Another impact is the police visiting the home or work address of an individual with no link to an investigation. This occurred in 7 of the 24 cases with 10 people affected. The final example given by the IPCO is a delay in a welfare check on an individual who is potentially at risk such as a young person at risk of sexual exploitation because the wrong addresses were investigated.[16]

The IPCO gives two key takeaways from these errors. First, the fact that the majority of serious errors were a result of human error (20 of 24) with the remaining 4 derived from system or technical errors. The human error cases included instances where data was misinterpreted and when data was entered incorrectly.[17] The second key takeaway is that errors in this context can have grave consequences for the victim of the mistake, together with their family and friends. The report highlights that this is particularly evident when homes or offices are searched and the nature of the investigation is revealed to an individual's family, neighbours or employers. Children may be taken into care, jobs may be suspended or dismissed, and bail conditions may force a person to leave their home.

One particular case is simply described in the report as a misinterpretation of data, which led to an innocent person being arrested and interviewed for the crime of uploading indecent images of children. An IP address had been found by the bulk authority which shared such images. This information was shared with the corresponding police force and a warrant was drawn up to arrest the owner of said IP address. However, when South Hertfordshire police requested details about the IP address in question they added an extra digit by mistake. This new erroneous IP address led South Yorkshire police to Nigel Lang's door.[18] While this is written up in the report as simply causing an innocent person to be arrested and interviewed,[19]

[15] Investigatory Powers Commissioner's Office, *Annual Report*, (2018) para 14.29.
[16] Ibid para 14.33.
[17] Ibid para 14.32.
[18] Champion M, 'This is what it's like to be wrongly accused of being a paedophile because of a typo by police' *Buzzfeed News* (https://wzfeed.com/matthewchampion/this-mans-life-was-destroyed-by-a-police-typo.
[19] Investigatory Powers Commissioner's Office, *Annual Report*, (2018) p116.

the false accusation of Lang being a paedophile had more serious consequences. He was subject to strict bail conditions and was forbidden to live with his family, visit his son there, or have any unsupervised contact with his son anywhere. Despite his innocence his arrest for possessing and distributing indecent images of children was still on file, as was his DNA.

After an investigatory process by his solicitor revealed South Hertfordshire Police's mistake the details of his arrest were altered so that they would not be disclosed to future employers. Following the admission of this mistake Lang sought compensation for a breach of the Data Protection Act 1998, false imprisonment, police assault/battery and trespass by police. In 2016 South Hertfordshire settled out of court for £60,000. Prior to his arrest Lang had no history of mental health problems but as of 2017 he was on antidepressants and had been diagnosed with PTSD.

While Lang's case is a particularly severe one it points to a larger problem with bulk surveillance errors. As surveillance is invoked to stop serious crime or for national security purposes, the consequences for those accused are quite severe. Therefore, there must be an exceedingly narrow margin of error in the operation of surveillance. This may be possible for targeted surveillance operations as a closer inspection of the target may reveal their innocence prior to any concrete action by the authorities. However bulk surveillance gathers far too much data to countenance even a narrow margin of error. It is not stated how South Hertfordshire police found this IP address which shared indecent images of children but it isn't beyond possibility that it was picked up by a bulk interception operation. This was then shared with another police force who acted upon it in good faith. The impact this small error had on Lang's life was huge. There is also a need for effective mechanisms in place to identify such errors, as following the failure to find indecent images on Lang's computer the IP address could have been checked and the error found. Another case concerning the sharing of indecent images of children led to a family being mistakenly visited by police three times only to find that an examination of the router found "an anomaly with the IP address assigned to it" due to crossed wires in the street furniture. This led to the IP address of one house being swapped with another. During this six-month period the family's computer was seized and their children were taken into protective custody.[20]

Returning to the issue of transparency, the difference in understanding between the reader of the IPCO's report and those who read the news article on Lang's case is substantial.

[20] Investigatory Powers Commissioner's Office, *Annual Report*, (2018) p 123.

Admittedly it would not be advisable for the report to name Lang as it would be a further invasion of his privacy but clearly the description of a misinterpretation of data leading to a false arrest does not adequately convey the potential harm of a serious error. This section shows that efforts should be made to move past a reliance on statistic and macro level transparency reporting and move towards the meso or micro level where anonymised accounts of serious errors and the procedures and safeguarding mechanisms utilised by the SIAs to account for them. While transparency requires that the public know to what extent these powers are used and how the SIAs normally use them, it also requires that the public sees how the SIAs misuse said powers and how they are held accountable by oversight mechanisms such as the IPC and IPT.

9.5 The Investigatory Powers Tribunal: An issue of substantive and procedural justice

9.5.1 IPT: Reporting

To determine the effectiveness of the IPT as a supervisory body it is instructive to examine the IPT's own reporting of its judgments before taking a closer look at certain cases. Until 2016, the IPT provided reports on the number of complaints it received and the outcomes by year. However, following a FOI request made by the author of this thesis, it was discovered that the IPT has not produced a report since 2016. The following table summarises the data that is currently available:

Year	New Cases Received	Cases Decided	Decision Breakdown
2010	164	210	99 (47.1%) received a no determination outcome
			65 (30.9%) were ruled as frivolous or vexatious
			18 (8.5%) were ruled out of jurisdiction
			15 (7.1%) were ruled out of time
			6 (2.8%) found in favour
			4 (1.9%) case dismissed
			3 (1.4) were withdrawn
2011	180	196	86 (43.8%) were ruled as frivolous or vexatious
			72 (36.7%) received a no determination outcome
			20 (10.2%) were ruled out of jurisdiction
			11 (5.61%) were ruled out of time
			3 (1.5%) were withdrawn

			2 (1.0%) were judged to be not a valid complaint
			2 (1.0%) were found in favour
2012	168	191	100 (52.5%) were ruled as 'frivolous or vexatious'
			62 (32.5%) received a 'no determination' outcome
			14 (7.3%) were ruled out of jurisdiction
			9 (4.7%) were ruled out of time
			5 (2.5%) were withdrawn
			1 (0.5%) were judged to be not a valid complaint
2013	205	161	85 (52.8%) were ruled as frivolous or vexatious
			50 (31.0%) received a 'no determination' outcome
			17 (10.5%) were ruled out of jurisdiction, withdrawn or not valid
			9 (5.5%) were ruled out of time
2014	215	201	104 (51.7%) were ruled as frivolous or vexatious
			53 (26.3%) received a no determination outcome
			36 (17.9%) were ruled out of jurisdiction, withdrawn or not valid
			8 (3.98%) were ruled out of time
2015	251	219	101 (46.1%) were ruled as frivolous or vexatious
			65 (29.6%) received a no determination outcome
			38 (17.3%) were ruled out of jurisdiction, withdrawn or not valid
			7 (3.2%) were ruled out of time
			8 (3.6%) were found in favour
2016	209	230	120 (52.1%) were ruled as frivolous or vexatious
			58 (25.2%) received a no determination outcome
			26 (11.3%) were ruled out of jurisdiction, withdrawn or not valid
			11 (4.7%) were ruled out of time
			15 (6.5%) were found in favour

Table 2: IPT Cases Decided 2010-2016

In the above table a ‘no determination’ outcome means that either the Tribunal was satisfied that there had been no conduct in relation to the complainant by any relevant body under the jurisdiction of the Tribunal, or that there had been some activity but it was not in contravention of the relevant legislation and so could not be determined as unlawful. The Tribunal is not permitted under RIPA to disclose whether or not complainants are or have been of interest to SIAs or law enforcement agencies. The Tribunal is also not permitted to disclose what evidence it took into account when considering the complaint.[21]

[21] Investigatory Powers Tribunal Report 2010 p 16

A ‘frivolous or vexatious’ ruling occurs where the IPT concludes that the complaint is obviously unsustainable and/or vexatious. A complaint is obviously unsustainable where it is so far-fetched or ill-founded as to justify said description. A complaint is vexatious where it is a repetition of an earlier obviously unsustainable complaint by the same person. An ‘Out of Jurisdiction’ ruling is given where the Tribunal holds that it has no power to investigate the complaint. An ‘Out of Time’ ruling is given where the Tribunal rules that the complaint is out of time and the time limit should not be extended. A case is dismissed when, for example, the complainant has failed to comply with a request for information (after due warning).[22] With this in mind we can see the percentage make-up of the IPT’s rulings below.

Decision Breakdowns	Number	%
Frivolous or Vexatious	661	46.95
No Determination	459	32.60
Out of Jurisdiction, Withdrawn or Not Valid	183	13.00
Out of Time	70	4.97
Found in Favour	31	2.20
Dismissed	4	0.28
Total	1408	100

Table 3: Totals of IPT Judgment Outcomes 2010-2016

From these two tables we can see that the vast majority of rulings before the Tribunal – roughly 80% – were ruled to be either frivolous or vexatious or simply given no determination. Roughly 13% more were ruled to be outside the IPT’s jurisdiction, were withdrawn by the complainant or held to be not valid. A further 5% were ruled to be out of time and 0.28% of cases dismissed in the course of an investigation, leaving just 2.2% found in favour of the complainant – only 31 rulings in the course of seven years. This could suggest that it is difficult to bring a complaint to the IPT successfully, although the Table admittedly does not give us a clear picture of the substance of the complaints that were submitted to the Tribunal. There is an observable increase in favourable rulings in 2015/2016 which lines up with the introduction of the IPA in 2016 but without any subsequent reports from the Tribunal it is difficult to ascertain whether this trend continues.

[22] ibid

While it would be easy to point to the above statistics as evidence of the inadequacy of the IPT as a remedy, it is equally easy to explain the figures away, especially given the lack of transparency surrounding the individual judgments. First, the very low rate (2.2%) of cases found in favour of the complainant may be indicative of the quality of complaints the Tribunal receives. Access to the Tribunal is free, and it is not difficult to imagine a person who believes they are subject to surveillance, with little to no evidence, making repeated complaints which are then ruled as 'frivolous or vexatious' (46.9%). Still, this doesn't account for the 32.9% which receive a 'no determination' outcome. Another explanation which does explain the prevalence of 'no determination' outcomes is simply that less people are subjected to surveillance than suspected. This seems unlikely given the scope and breadth of the legal powers described here and the technology described in chapter one. The volume of communications intercepted by bulk methods means this possibility is slim. However, these obfuscations still stand and, in combination with the justifications accepted by the Court in *Kennedy,* make arguing against the effectiveness of the IPT based on outcomes difficult.[23] A more fruitful path is to examine the lack of procedural justice present in the IPT's proceedings.

9.5.2 Procedural Justice, the IPT and Article 6 ECHR

It is clear from the tables above that the IPT very rarely decides an outcome in the claimant's favour. However, considering the covert nature of the investigatory powers and that many submit claims without knowing for sure that their communications have been intercepted, perhaps this is to be expected. Given these barriers to further empirical investigation, it is better to focus on the procedural justice of the IPT's proceedings. Studies have repeatedly found that when people come into contact with the law, they care not only about the outcome but also how it was handled. The perception of procedural justice is a more significant factor determining the perception of legitimacy of the institution concerned than the perception of distributive justice, or the outcome.[24] Traditional models of procedural justice focus on two key antecedents: the quality of decision making and the quality of interpersonal treatment. Models of motive-based trust emphasise these antecedents and add others, such as whether people say they understand why the authorities acted as they did and whether they say they share social bonds with the authorities. Trust and procedural justice are then intertwined as

[23] See Kennedy discussion in Chapter 3.
[24] Tom R. Tyler. "Procedural Justice, Legitimacy, and the Effective Rule of Law." (2003) 30 Crime and Justice 284

people perceive procedures enacted by those they trust to be fairer, and authorities become trusted when they are seen to exercise their authority fairly.[25]

In Thibaut and Walkers's early discussions of procedural justice they emphasise the importance of participation in the process as an antecedent to procedural justice.[26] The logic behind this is that people are more satisfied with a procedure that allows them to participate, explain their side of the story, and communicate their views on how the matter should be resolved.[27] Tyler and Huo's work suggests that while participation does not independently influence assessments of procedural justice, it does have an important indirect influence on such assessments.[28] People are more likely to rate the quality of decision-making highly when the procedure allows them opportunities to participate.[29] This lines up with Lord Reed's statement in *Osborn* that, "justice is intuitively understood to require a procedure which pays due respect to persons whose rights are significantly affected".[30] Walden links participation to dignity in that those affected by the decision should be respected "as beings capable of explaining themselves".[31]

Brems and Lavrysen derive four criteria for procedural justice in the context of human rights adjudication in the ECtHR: participation, neutrality, respect and trust. For the participation criterion, people must have formal participation: "the opportunity to tell their side of the story in their own words before decisions are made."[32] This has a positive effect regardless of outcome, as long as the claimant feels that authority sincerely considered their argument before making their decision. This participation is thus not simply formal but substantive as citizens must also infer that their views are being considered by the decision-maker. For the neutrality criterion, judges must act as "neutral, principled decision makers who make decisions based on rules and not personal opinions".[33] This relates to the perception of

[25] Ibid p. 300
[26] John W Thibaut,., and Lauren Walker. 1975. Procedural Justice: A Psychological Analysis. Hillsdale, N.J.: Erlbaum.
[27] John W Thibaut., and Lauren Walker. 1975. Procedural Justice: A Psychological Analysis. Hillsdale, N.J.: Erlbaum.
[28] Tom R Tyler, and Yuen J. Huo. 2002. Trust in the Law: Encouraging Public Cooperation with the Police and Courts. New York: Russell-Sage Foundation.
[29] Tom R. Tyler. "Procedural Justice, Legitimacy, and the Effective Rule of Law." (2003) 30 Crime and Justice 283, 300.
[30] *Osborn v. The Parole Board* [2013] UKSC 61, paras. 67 - 72
[31] Jeremy Waldron, 'How Law Protects Dignity' [2012] 71 CLJ 200 p. 210
[32] Eva Brems and Laurens Lavrysen. "Procedural justice in human rights adjudication: The European Court of Human Rights." *Human Rights Quarterly* (2013): 180.
[33] Ibid 181.

independence and impartiality of the judge, and equal treatment to all parties. This criterion also includes transparency, and consistency in the application of the law. For the respect criterion, people need to be treated with dignity and respect and should feel like their concerns are being taken seriously. For the trust criterion, there must be an assessment of the character of the decision maker. Citizens make motive attributions on whether the officials involved are motivated to be just.[34]

This focus on procedural justice is manifest throughout the ECHR. It is most prominent in Article 6 case law wherein these criteria form part of the fair trial requirements, but it has also been invoked consistently under the Article 8 right to family life. Additionally, these criteria have been either directly or indirectly invoked in the areas of planning and environment,[35] deprivation of legal capacity,[36] data registration[37], registration of ethnic identity[38] and access to abortion.[39] The legality requirement, which the Court often relies on in cases where the Contracting State has been given a wide margin of appreciation, also contains a substantial aspect of procedural justice. This was integrated into the test in the *Al-Nashif v. Bulgaria* case.[40] The Court held that the requirement that an interference with a human right must have a legal basis must include a requirement of compatibility with the rule of law. Therefore, the provision of a measure of legal protection in domestic law against arbitrary interference by public authorities is required. The Court clarified that this includes national security cases as:

> the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence.[41]

[34] Ibid.
[35] *Hatton v UK,* (2003) 37 EHRR 611; *Buckley v United Kingdom*, (1997) EHRR 101; *Taskin v. Turkey*, (2006) 42 EHRR 50.
[36] *Shtukaturov v. Russia*, App no 44009/05 (ECtHR 27 March 2008); *Salontaji-Drobnjak v. Serbia,* App. No. 36500/05 (ECtHR 13 October 2009).
[37] *Turek v. Slovakia,* App. No. 57986/00 (ECtHR 14 February 2006).
[38] *Ciubotaru v. Moldava*, App. No. 27138/04 (ECtHR 27 April 2010).
[39] *Tysiac,* App. No. 5410/03 (ECtHR 20 March 2007).
[40] Eva Brems and Laurens Lavrysen. "Procedural justice in human rights adjudication: The European Court of Human Rights." *Human Rights Quarterly* (2013): 176-200.
[41] *Al-Nashif,* App. No. 50963/99 123.

In this way, there is tension between the IPT and the foundational aspects of Article 6 ECHR.[42] For example, the requirement that the fair administration of justice should be conducted via an open procedure. While the Court has allowed for the qualification of this requirement, such as in national security contexts, the Court has also reiterated the importance of public proceedings in protecting complainants against the administration of justice with no public scrutiny.[43] Further, the Court emphasised that public proceedings are the measure which ensures the preservation of trust in the courts.[44] It should be noted that under the updated Tribunal Rules, the IPT must endeavour – to the extent that is consistent with its public interest mandate – to conduct proceedings in public and in the presence of the complainant.[45] This is a positive development, even if the IPT remains under no duty to hold an open hearing, as it is an attempt to "prevent public interest considerations overriding individual rights without a balanced consideration of both sides".[46]

The IPT's ability to conduct closed hearings interferes with the Article 6 principle of equality of arms as it impedes the ability of complainants to present an effective case. If the Tribunal conducts a closed hearing then complainants cannot be informed of arguments made or see the evidence adduced by a public authority where to do so would entail a risk to national security.[47] In this way the spectre of Closed Material Procedure (CMP) again haunts the IPT, in which efforts are made to preserve the equality of arms between the parties. Most applicable here would be the use of Special Advocates under CMP. Whilst the use of Special Advocates remains controversial – Lord Neuberger in *Bank Mellat*, for example, commented that "any judge … must regard the prospect of a closed material procedure, whenever it is mooted and however understandable the reasons it is proposed, with distaste and concern"[48] – the appointment of a Special Advocate at least represents an attempt to ensure equality of arms between the parties, which is missing in the IPT. Where special counsel have been appointed, their role has been limited to akin to that of amicus curiae, meaning that they assist the Tribunal itself rather than the complainant. They may assist the complainant, but they are

[42] Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129 p 135.
[43] *Martinie v France* App no 58675/00 (Grand Chamber, 12 April 2006) para 39.
[44] Ibid.
[45] IPT Rules 2018 (n 9), Rule 10(4).
[46] Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129 p 136.
[47] Ferguson, G and Wadham, J "Privacy and surveillance: a review of the Regulation of the Investigatory Powers Act 2000" EHRLR. 2003, Supp (Special issue: privacy 2003), 101 – 108.
[48] *Bank Mellat v HM Treasury (No.2)* [2014] AC 700 para 51.

not required to do so.[49] This then appears to be a missed opportunity for the Tribunal, who could appoint a Special Advocate for the complainant should they need to conduct a closed hearing. This topic will be returned to in a later section. Prior to that it is useful to see if this proclaimed lack of procedural justice is present in the IPT case law.

9.5.3 IPT Cases: An overview

From reading the cases the IPT has decided to publish it seems like there are several broad categories which they fall into. Each of these categories carries with it a different procedure and thus a different amount of procedural justice. The first category is the use of investigatory powers by organisations which are not SIAs such as the police and local councils. This is the category where the Tribunal's potential as an effective domestic remedy is maximised. For example, there is the *Paton* case concerning a local council's use of surveillance powers for a non-legitimate aim.[50] Another council case is *Vaughan v South Oxfordshire District Council*[51] concerning whether the inspection of property constituted covert surveillance under RIPA. While the complainant was unsuccessful, the Tribunal provided him with an equality of arms. As he had no legal representation they assigned him a QC to represent him. All evidence was available to be examined. The Tribunal also gave clear and thorough reasoning as to why the overt act of inspecting property during the day could not be considered to be covert surveillance under RIPA.

Also within this first category are a number of cases concerning police leaks and journalistic sources. In the *Police Scotland*[52] case the respondent police chief conceded that there had been unlawful interception of the communications of the police officers, and by extension their partners and families, based on the suspicion that said officers had been leaking details of an ongoing murder investigation to the press. Interestingly, the initial complaint in *Police Scotland* stemmed from the Interception of Communications Commissioner spotting the misuse of investigatory powers in their review and contacting the complainants. The report concluded that the purpose of the interception was to determine either a journalistic source or one acting as an intermediary between a source and a journalist, this was held to be an

[49] Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129 p 137.
[50] *Paton and others v Poole Borough Council* [2010] (IPT/09/01. 02. .03. 04 and 05).
[51] *Vaughan v South Oxfordshire District Council* [2012] IPT/12/28/C.
[52] *Police Scotland* [2016] UKIPTrib15_602-CH.

unlawful use of the powers in question.[53] The *News Group* case[54] also concerned the interception of police officers' communications who were suspected of leaking to the press, as did *Dias and Matthews v Cleveland Police*.[55] Other police related cases included *Davies v British Transport Police*,[56] concerning unauthorised directed surveillance on a train, *Chatwani v National Crime Agency*[57] concerning the bugging of a house without accounting for the risk of capturing LPP, and *AB v Hampshire Constabulary*,[58] concerning being recorded by police body cam without consent.

Generally, the efficacy of the Tribunal as a remedy is high in these cases. While the police aim to pursue to the legitimate aims of protecting public health or morals or preventing serious crime, they are not permitted by the Tribunal to hide behind this legitimate aim through the use of a 'neither confirm nor deny' (NCND) policy. The Tribunal is then able to allow the complainant to participate fully in the proceedings while sitting as a neutral arbiter of the decision, as the cases were not heard in closed session. In this way the complainant is treated with respect and can trust in the Tribunal irrespective of the outcome. It seems that in terms of procedural justice the IPT is capable of dealing with cases of overt surveillance.

Another category of cases is ones concerning claims against surveillance legislation *in abstracto* by NGOs such as Amnesty International, Big Brother Watch, and Privacy International. These are more difficult to evaluate as there is no specific grievance for the IPT to seek to remedy. Rather, in these instances the IPT acts as a functional lower court to the ECtHR as complainants submit that various aspects of the surveillance regime are incompatible with Articles 6, 8, and 10 ECHR. Here the IPT acknowledges the difficulty in establishing victim status in bulk surveillance cases as complainants find it difficult to prove that their communications have been subject to one of the bulk powers. In these cases the Tribunal proceeds on the basis of 'assumed facts' or 'factual premises': facts which are agreed upon by the parties but not confirmed by the intelligence services. While this is not conducive to the complainants knowing whether they have actually been subject to surveillance, that is not the purpose of their bringing a complaint. Rather, it enables the Tribunal to proceed with the complainants' submitted issues – generally the compatibility of

[53] Ibid para 27.
[54] *News Group* [2015] UKIPTrib 14_176-H.
[55] *Dias and Matthews v Cleveland Police* [2017] UKIPTrib 15_586-CH.
[56] *Davies v British Transport Police* [2018] UKIPTrib IPT_17_93-H.
[57] *Chatwani v National Crime Agency* [2015] UKIPTrib 15_84_88-CH.
[58] *AB v Hampshire Constabulary* [2019] UKIPTrib 17_191-C.

bulk surveillance measures – without consideration for national security. Cases in this category include *Privacy International & Greennet*,[59] *Liberty*[60] and *Human Rights Watch*,[61] each of which was brought before the Tribunal in light of the Snowden revelations. In *Liberty* the complainants specifically challenged the compatibility of the Prism and Upstream surveillance programmes with Articles 8 and 10 ECHR. GCHQ's involvement in these programmes was subject to the Neither Confirm Nor Deny policy, but the IPT allowed the complaint to proceed on the assumed facts that GCHQ had been involved in these programmes.[62] As the purpose of the complaint concerns the compatibility of these measures with the ECHR, the IPT's willingness to bypass the NCND policy is essential to allowing the complainants to participate meaningfully.

However, it should be noted that in *Liberty* the Tribunal did conduct two closed hearings with the respondents in the course of the proceedings, which excluded the complainants.[63] The IPT attempted to account for this exclusion through the use of a Counsel to the Tribunal acting as amicus curiae. The Counsel distinguished its own role from that of a Special Advocate, specifically the lack of partisanship on the part of the Counsel. The Counsel accounted for this lack of representation by the fact that both the complainants and respondents agreed that Counsel to the Tribunal was best suited to assist in this disclosure role.[64] While this may have alleviated the lack of representation for the complainants, it is unclear if a Special Advocate would have been implemented had the complainants been opposed to this lack of representation. This tension between Special Advocates and amicus curiae will be returned to later in this chapter.

Where the IPT's flaws, in terms of procedural justice, begin to show is when they have to consider the SIAs, and by extension the executive. In this third category of cases, the primary cause for this seems to be the invocation of the 'neither confirm nor deny policy (NCND), a mechanism which seeks to avoid potential risks to national security that could be caused by either confirming or denying the information's existence. This should be considered a step further towards secret justice than CMP as at least under CMP the complainant can confirm that such information on them exists even if they cannot themselves obtain it. Under NCND,

[59] *Privacy International & Greennet* [2016] UKIPTrib 14_85-CH.
[60] *Liberty* [2014] UKIPTrib 13_77-H.
[61] *Human Rights Watch* [2016] UKIPTrib 15_165-CH.
[62] *Liberty* [2014] UKIPTrib 13_77-H para 4.
[63] Ibid para 7.
[64] Ibid para 10.

the existence of this information is uncertain. This not only means that the complainant cannot examine it, but also the IPT finds itself bound to make a decision based on either a small amount of information, or government affirmations.[65] Without access to independent sources of information, or their own intelligence service, it is very difficult for the court to challenge the executive on a sure footing as they are not in possession of all the information leading to the decision.[66] The full implications of which can be found in the *Steiner* and *Belhadj* cases discussed below.

9.5.4 Contrasting Three IPT Cases

The following section aims to elucidate the previous section by highlighting the differences between three cases before the Tribunal. The first, *Paton*, highlights the exemplary level of procedural justice the IPT can deploy in cases concerning surveillance by public bodies such as Poole Council.[67] The second, *Belhadj*, evidences the lower level of procedural justice in cases concerning the operation of SIAs and national security.[68] The third, *Steiner*, shows the lack of procedural justice present in proceedings concerning SIAs even without national security considerations.[69]

Paton[70] provides a good example of the levels of procedural justice the IPT is capable of providing. Following a complaint from members of the public that the applicant had used a fraudulent address to obtain a school place for one of her children, Poole Borough Council applied for directed surveillance authorisation.[71] The Tribunal first examined issues with the authorisation of surveillance. This included the fact that the application had stated that the address information provided to the Council by the applicant was fraudulent, yet the point of the surveillance was to ascertain whether this was in fact the case.[72] Other issues included three young children as targets of surveillance,[73] misstatement of the appropriate test for

[65] Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129.
[66] Aileen Kavanagh, 'Constitutionalism, Counterterrorism, and the Courts: Changes in the British Constitutional Landscape' (2011) 9(1) IJCL 172-199, 178.
[67] *Paton and others v Poole Borough Council* [2010] (IPT/09/01. 02. .03. 04 and 05).
[68] *Belhadj v Security Service* [2015] UKIPTrib 13_132-H.
[69] *Vincent C Frank-Steiner v the Secret Intelligence Service* [2008] (IPT/06/81).
[70] *Paton and others v Poole Borough Council* [2010] (IPT/09/01. 02. .03. 04 and 05).
[71] Ibid para 12.
[72] ibid para 23.
[73] ibid para 58.

'ordinary residence',[74] and the application being out of time.[75] The surveillance itself lasted for roughly one month and involved driving by the two residences in question, monitoring the property from a parked car and following the applicant and her children. The Council concluded that on balance the applicant's information wasn't fraudulent.

In deciding the case the Tribunal asked itself three questions regarding the authorisation of directed surveillance: the purpose of the authorisation, the necessity of the authorisation and the proportionality of the authorisation. Regarding the purpose of the authorisation, the Council did not identify a crime to be prevented or detected - the only sanction given for providing misinformation in a school application was denial of a place at the school. So, the purpose was to detect if the family were living in the catchment area. The Tribunal thus concluded that the Council had not established that the surveillance was for the purpose of preventing or detecting crime.[76] Regarding necessity, the Tribunal asked if the person authorising the surveillance believed it was necessary on the grounds of preventing or detecting crime.[77] The fact that the entire family was subjected to surveillance with no separate consideration for the children, and that for the father and three children there was clearly no actual or potential criminal offence, caused the Tribunal to hold that the person providing authorisation should have considered this and found the surveillance to be not necessary.[78] Regarding the proportionality of the measure, the fact that children were targeted and the authorisation was out of time caused the Tribunal to conclude that the surveillance was not proportionate and could not reasonably have been believed to be proportionate.[79] Thus, the Tribunal found a violation of the applicant's Article 8 rights.[80] In terms of procedural justice, the particulars of Paton's case were discussed and the actions of the council were subjected to a necessity and proportionality test. The manner in which Paton's case was treated meant that she was far more likely to trust in the outcome as she was able to meaningfully participate in the deliberations of a neutral tribunal which conducted a thorough review.

[74] ibid para 57.
[75] Ibid para 59.
[76] ibid para 63.
[77] Ibid para 66.
[78] Ibid para 69.
[79] Ibid para 73.
[80] Ibid para 85.

In *Belhadj*, the applicant had little meaningful opportunity to participate. This lack of participation is stark when compared with *Patton*. *Belhadj* concerned the declaration by the IPT in a previous case that the statutory regime under RIPA for the interception of legally privileged material (LPM) was unlawful.[81] Having found this, the question in *Belhadj* was as follows: if the IPT found that there had in fact been interception of legally privileged material, would it be obliged to make a determination in favour of those affected? Subsequently, the IPT conducted a closed procedure "in which consideration of any documents and information relating to any legally privileged material relating to any of the Claimants intercepted or obtained by the Respondents has taken place."[82] The eight claimants alleged that the respondent SIAs and Secretary of State had unlawfully intercepted communications that were subject to LPP. The respondents conceded that the regime for intercepting such communications was unlawful. The Tribunal made the appropriate declaration of incompatibility with Article 8(2) ECHR, then held a closed hearing to determine whether claimants' communications had in fact been intercepted.

The claimants argued that as the regime had been declared unlawful, the Tribunal was obliged to make a determination in the claimant's favour upon finding that interception of such material had taken place. The claimants argued that the IPT would then have to provide reasons for this determination, including findings of fact.[83] They also submitted that the SIAs' NCND principle was not applicable, or at least diminished, once the Tribunal found an unlawful act or a contravention of Article 8 ECHR.[84] The respondents argued that where the IPT has already made a systemic determination, and where making individual determinations would reveal that interception had in fact occurred, the Tribunal should only make a systemic determination. As an alternative they argued that if the Tribunal were to make an individual determination they should add the qualifier that the complainant's communications might have been subject to interception.[85] They also submitted that even if a determination was made in a claimant's favour, either no reasons or at most an abbreviated summary should be provided, in order to comply with the IPT's duty not to disclose information prejudicial to national security.[86]

[81] *Belhadj v Security Service* [2014] UKIPTrib 13_132-9H.
[82] *Belhadj v Security Service* [2015] UKIPTrib 13_132-H para 4.
[83] Ibid para 6.
[84] Ibid para 16.
[85] Ibid para 7.
[86] Investigatory Powers Tribunal Rules 2000 r.6(1).

This was a step too far for the IPT who found in favour of the claimants. The Tribunal considered it contrary to the interests of the public and inconsistent with public confidence in the IPT to find in favour of the respondents. The IPT is trusted to investigate matters, which is often done in closed proceedings. If the meaning of a 'no determination' outcome was extended to mean *either* there has been no interception *or* there has been lawful interception *or* there has been unlawful interception, the resultant level of ambiguity would place the validity of all the IPT's decisions into doubt. Further, to conceal findings of unlawful conduct on the basis of a non-specific submission of risk to public safety would undermine public confidence that Parliament had created a means of holding the relevant public agencies to account.[87] The respondents' stance on this issue shows the difficulties the IPT faces in their attempts to hold the SIAs to account. If the IPT simply kowtowed to the SIAs it would obfuscate whether or not surveillance had taken place further.

This did not mean that the IPT was in favour of the claimant's submission that NCND should be inapplicable when unlawful interception has been found. Rather, the NCND policy might have a role to play in the giving or abbreviating of the reasons or information to be supplied following a determination in the complainant's favour. Here, the Tribunal had regard to the fact that disclosure could have very damaging effects on the SIA's ability to protect the public. However, if the making of a determination in the complainant's favour disclosed that there had been interference with his ECHR rights, that was a consequence of the contravention and could not be avoided.[88] With this in mind the Tribunal concluded that a determination should be made but only in favour of one of the claimants, and only in respect of two documents.[89]

Belhadj is emblematic of the bind the IPT finds itself in generally when it comes to national security and the SIAs. First, it has complainants seeking a remedy for the possible infringement of their ECHR rights who, due to the covert nature of surveillance, have no evidence that this has occurred. The Tribunal is tasked with acting as an investigator for them, accessing information which they are unable to ever see for themselves and providing them with an effective domestic remedy. Second, the Tribunal is tasked, by Parliament, to hold these SIAs (and more broadly the executive) accountable in their use of investigatory powers while simultaneously safeguarding the work of the SIAs. Third, as a judicial entity

[87] *Belhadj v Security Service* [2015] UKIPTrib 13_132-H para 19.
[88] Ibid para 21.
[89] Ibid para 22.

the Tribunal itself has a general duty to hold up the rule of law. The tensions between these considerations played out in *Belhadj*. The Court rejected the SIA's argument that no determination outcomes should be made even more ambiguous in the name of national security, but also rejected the argument that NCND should not apply in cases of unlawful interception. In this way the IPT attempted to reconcile the competing interests by making a determination in the claimants' favour, revealing how and what was intercepted, but limiting this disclosure to only two documents about one of the nine claimants. It is difficult to see how the IPT has satisfied either party with this outcome but at the same time it is equally - if not more - difficult to see how they could have gone further, given the circumstances in which it operates.

In terms of procedural justice, the flaws in the Tribunal's approach begin to appear, especially so when compared to *Paton*. In terms of meaningfully participating, the complainants are fully excluded from the closed hearing on which the complaint hinges. While there is little need for the presence of the complainants in order to answer the investigatory question of whether surveillance occurred, on the question of whether details of the surveillance should be disclosed, representation of the complainants is required for meaningful participation. The complainants could have been provided with partially redacted summaries of the documents in question or a special counsel could have been appointed to them. Neither are substitutes for meaningful participation, but they would alleviate some of the issues the IPT faces here. Regarding neutrality, it is arguable that the Tribunal was attempting to balance considerations between the SIAs and complainants, but to the complainants it could be reasonably construed as the IPT being biased in favour of the SIAs due to its legislative obligations. These two factors would have impacted the respect the complainants felt from the proceedings and the trust they had in them.

Steiner[90] demonstrates the lack of procedural justice found in the IPT's approach in cases concerning SIAs, even without national security considerations. The *Steiner* ruling also provides a good example of the no determination outcome occurring in practice. The applicant challenged the lawfulness of MI6 keeping secret records on the applicant's uncle. The applicant claimed that said uncle was a spy for Britain during WW2 and made an Article 8 claim regarding the right to respect for private and family life.[91] The Tribunal rejected the

[90] *Vincent C Frank-Steiner v the Secret Intelligence Service* [2008] (IPT/06/81).
[91] Ibid para 1.

Article 8 claim as the family member in question was long dead and had never formed part of the complainant's household.[92] The second claim regarded judicial review of MI6's conduct in refusing to disclose whether there were any documents on the complainant's uncle and, if there were any, to allow inspection of them.[93] The Tribunal reserved the right to inspect these files, if they existed. Thus, the Tribunal concluded that it would investigate if said files existed. They set out that if no files existed then a no determination outcome would be appropriate. If the files in question existed then the Tribunal would consider first whether it was reasonable for MI6 to conclude that it didn't have the grounds to disclose said files in the interest of national security, then it would consider whether it was reasonable for MI6 to not transfer such documents to the National Archives. If the Tribunal was satisfied on both counts, then they would also give a 'no determination' outcome. Subsequently the applicant received a no determination outcome.[94]

While it is generally accepted that a no determination outcome may sometimes be required on national security grounds, arguably it is difficult to justify in *Steiner*. Given that the information in question pertained to a long since deceased individual who may or may not have worked as a spy for MI6 during World War II, it is difficult to see what national security considerations may arise from disclosing this information. The no determination outcome is particularly frustrating as it is impossible to know whether the files in question exist or not. While the applicant was allowed to participate in the proceedings, it is debatable whether this constituted meaningful participation. Was there anything that the applicant could have said or done to persuade the IPT to disclose said information or even to confirm that Steiner's relative was or was not a spy? Likewise, it is not clear whether the weight which is placed on keeping the work of the SIAs secret allows the Tribunal to appear sufficiently neutral in its deliberations. With regard to the respect and trust criteria, once the Tribunal informed Steiner that they would investigate the files in question if they existed – but that he would only be told whether or not they existed if they did exist *and* it was unreasonable for MI6 to refuse to disclose them on national security grounds – one can imagine that Steiner would have concluded that his chances of success were exceedingly slim. Further, as explained above, the fact that the test is whether it is reasonable for MI6 to conclude that non-disclosure is in the interests of national security tips the scales in the SIA's favour. If the test applied by the

[92] Ibid para 10.
[93] Ibid para 16.

Tribunal asked whether non-disclosure is necessary for the purposes of national security, the outcome of a case like *Steiner* might have been different and Steiner himself would have had a greater sense of the importance of not disclosing the requested information.

These three cases were chosen for closer examination as they are emblematic of the differing roles the IPT can take depending on the context of the case before them. The differing levels of procedural justice present in *Paton, Belhadj,* and *Steiner* show how the IPT's effectiveness as a safeguard against abuse can vary between cases, particularly where the IPT must interact with the use of investigatory powers by the SIAs. These issues seem to stem from the use of closed sessions. While *Paton* did not have a closed session, *Belhadj* and *Steiner* did. In the latter two cases the complainants had no representation in the most important part of their cases. In *Belhadj* this closed session led to a very limited disclosure of the requested information. In *Steiner* it led to no disclosure at all. While the legitimate aim of national security will play a role in the level of procedural justice the IPT can achieve, in particular the necessity of closed sessions, there are mechanisms which can be implemented to improve it, namely the disclosure of information procedures under PII and the use of Special Advocates.

9.6 Public Interest Immunity, Special Advocates and the IPT

Perhaps the most direct comparator for the IPT is the Public Interest Immunity mechanism (PII). Both concern qualifications to the rule of law principle of a fair and open trial on the grounds of public interest such as national security, particularly the common law principle of open disclosure.[95] While PII and Special Advocates have both been subject to extensive criticism[96], it nonetheless arguably strikes a fairer balance between the public interest and the need to ensure a fair and open trial than the IPT.

9.6.1 Public Interest Immunity

Public Interest Immunity is an exclusionary mechanism developed in the common law wherein evidence may be excluded from proceedings. It is best explained through an examination of its stages as per *Wiley*.[97] First it must be considered whether the material which the public authority wishes to exclude is relevant to the legal proceedings.[98] Next, the

[95] Richard Glover, *Murphy on Evidence* (15th edn, OUP 2017) p 644.
[96] Cian Murphy. "Counter-terrorism and the culture of legality: the case of special advocates." (2013) 24 King's Law Journal 19-37., A Boon and S Nash, 'Special Advocacy: Political Expediency and Legal Roles in Modern Judicial Systems' (2006) 9 Legal Ethics 101.
[97] *Chief Constable of Midlands Police, ex parte Wiley* [1995] 1 AC 274.
[98] Ibid Lord Templeman p 5.

public authority in question must consider whether disclosure would entail a real risk of serious harm to an important public interest, such as national security.[99] Third, the public authority must decide whether, in its view, the public interest in non-disclosure outweighs the public interest in disclosure. If so, it will make a certificate to this effect.[100] Finally, the fourth stage is the court's assessment: the court is the ultimate decision-maker. In assessing the efforts of the public authority, the court will consider the alternatives to non-disclosure such as: redacted documents, summarised documents, confidentiality agreements, etc.[101] In this way, PII does not aim to balance the public interest against interference with a right - in this case the right to a fair trial - rather it frames each as a public interest in their own right. There is a public interest in the open and fair administration of justice, just as there is a public interest in national security.

This framing occurs throughout the use of PII. Bingham LJ held in *Makanjuola* that "where a litigant asserts that documents are immune from production or disclosure on public interest grounds he is not (if the claim is well founded) claiming a right but observing a duty".[102] While Bingham LJ was in the minority in *Makanjuola*, Lord Woolf in *Wiley* upheld this view as a "very clear statement as to the nature of public interest immunity"[103]. Lord Woolf later added that decisions to either disclose or to not disclose material are not conflicting decisions of public policy, but simply different aspects of public policy.[104] When the court upholds a disclosure decision, the aspect of public policy which favours the availability of information for use in litigation outweighs the competing aspect of public policy. While the IPT also conducts a balancing test in its proceedings, it is statutorily obliged to give more weight to the public interest of national security when balancing against interference with ECHR rights. This test can be summed up by reference to the IPT Rules 2018 which states that:

> The Tribunal must carry out their functions in such a way as to secure that information is not disclosed to a extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious

[99] Ibid.
[100] Ibid p 6.
[101] Ibid.
[102] *Makanjuola v Commissioner of Police of the Metropolis* [1992] 3 AII ER 617, 623.
[103] *Chief Constable of Midlands Police, ex parte Wiley* [1995] 1 AC 274.
[104] Ibid para 298.

crime, the economic interests of the United Kingdom or the continued discharge of the functions of any of the intelligence services[105]

This strong language can be contrasted with the other obligation upon the IPT: "the need to secure that matters which are the subject of proceedings, complaints or references brought before or made to the Tribunal are properly heard and considered."[106] This wording is noticeably weaker than the above quote and notably the need to properly hear and consider matters brought before it is not framed as a public interest in itself in contrast to the framing in the context of PII.

In instances where a decision has to be made whether or not to disclose information, the effect of this rule is to create a presumption in favour of non-disclosure. Unlike PII there is no mention of balancing two aspects of public policy. Rather the IPT must not act in a way which is contrary to the legitimate aims of national security, prevention of serious crime and the economic wellbeing of the UK. The IPT must also not act in a manner which is contrary to the public interest or the operation of the SIAs more generally. Further to this, the Tribunal may not generally disclose to the complainant, or any other person other than Counsel to the Tribunal:

(a) Any information or document disclosed or provided to the Tribunal in the course of a hearing;
(b) Any information or document otherwise disclosed or provided to the Tribunal by any person pursuant to section 68(6) RIPA or volunteered under 68(7)(a), effectively meaning any member of the state;
(c) Any information, document or opinion provided to the Tribunal by a relevant Commissioner
(d) The fact that any information, document, or opinion has been disclosed or provided in the circumstances mentioned in (a) to (c);
(e) The identity of any witness at a hearing, or the fact that any witness was called.[107]

The caveat is that the Tribunal may disclose anything outlined above if the relevant person gives their consent, the relevant person being a member of the executive, the SIA in question or a Judicial Commissioner.[108] If the person does not consent, then the IPT may require them

[105] Investigatory Powers Tribunal Rules s(7)(1).
[106] RIPA 2000 s(69)(6)(a).
[107] Ibid s7(2)(a-e).
[108] Ibid s7(3)(a-d).

to provide their reasons for their refusal and, after considering these reasons, direct the respondent to disclose the document or information, or to provide a gist or summary of the document/information. However, the respondent is free to refuse this direction, but then the Tribunal may direct them not to rely on the non-disclosed material in support of their case, or direct that the respondents must make such other concessions as the Tribunal may specify.[109] It is important to note the frequent use in these rules of the word 'may', indicating that discretion is vested in the IPT. If the IPT *may* direct the respondent not to rely on undisclosed material, it follows that it may also allow the respondents to do so. There is no discretion for the IPT to disclose material in circumstances where it disagrees with the executive as to the sensitivity of said materials. They are in fact prohibited from ordering any person to disclose information or documents which would be contrary to the public interest, prejudicial to national security or the other reasons listed above.[110] This compares unfavourably with PII procedure, in which applications for non-disclosure are subject to fairly intensive balancing considerations as well as a necessity test. Admittedly, the inherent covert nature of cases concerning SIAs may preclude a full transposition of PII balancing and the national security context may weaken the implementation of a necessity test. However, implementing even a partial version of the PII's exclusion of non-disclosed evidence safeguard would improve the fairness of the IPT's proceedings and their effectiveness as a domestic remedy. Partial in the sense that non-disclosed evidence should be inadmissible unless it is necessary to do otherwise, as opposed to PII's test of strict necessity.

Likewise, the IPT may disclose that they have held or intend to hold a hearing "(in whole or in part) in private or in the absence of the complainant".[111] The rules repeat that the decision to disclose the fact that a hearing has been or will be held without the complainant is subject to the general public interest duty outlined in the previous paragraph. This is an update from the IPT rules 2000 which held that the IPT may not generally disclose to the complainant or any other person that the Tribunal intends or has held an oral hearing in the absence of the complainant.[112] Additionally, the rules held that all the Tribunal's proceedings shall be conducted in private.[113] This was later rejected by the Tribunal in practice owing to fair trial concerns. Tomkins described the state of affairs under the 2000 Rules as: "a model, not

[109] Ibid s7(7)(b).
[110] Ibid s 7(10).
[111] Ibid s7(10).
[112] Investigatory Powers Tribunal Rules 2000 s6(2).
[113] Ibid.

merely of closed evidence, but which enables altogether secret justice."[114] It is difficult to disagree with him on this point, but it is not certain whether it still holds true for the IPT operating under the 2018 Rules. The 2018 Rules do not prohibit the IPT from holding open hearings but do allow them to hold closed hearings. There is leeway for the IPT to operate and often, as will be discussed in the case law section, the Tribunal splits cases into open hearings and closed hearings based on the non-disclosed material.

Another important safeguard for PII is that excluded evidence is inadmissible.[115] This is rooted in the principle that parties should disclose to each other any and all evidence relevant to the proceedings which is in their possession, custody or power.[116] The objective of this principle is that all such relevant evidence should be available to be inspected by all parties and that parties should be free to place before the court any evidence which will assist it in determining the truth and doing justice between the parties.[117] The necessary corollary rule to this is that no party should be entitled to frustrate or hinder the doing of justice by withholding from their opponent or from the court evidence which is relevant.[118] When a public authority invokes PII it effectively withholds from their opponent the ability to question the withheld evidence. Thus, in the interest of upholding equality of arms between the parties, the court will find such evidence to be inadmissible.

This corresponds to the strictness of PII. It has been stressed in multiple PII cases that disclosure of material should only be refused where it is strictly necessary to do so.[119] The court consults whether there are means of mitigating the effect of any restriction imposed on disclosure. Further, no immunity attaches to material simply because it was created and used confidentially, although the courts will respect confidentiality as much as possible.[120] In civil cases the court inspects the material in question and then balances the public interest in making them available for the purposes of litigation.[121] In criminal cases the court must regard the accused's right to a fair trial as the most important factor, while also considering the public interest in withholding information.[122] The general rule is that any material which

[114] Adam Tomkins, 'Justice and Security in the United Kingdom' (2014) 47 Isr L Rev 305 p 313.
[115] Joint Committee on Human Rights, 'The Justice and Security Green Paper' (London, 4 April 2012) p 91.
[116] Richard Glover, *Murphy on Evidence* (15th edn, OUP 2017) p 643.
[117] Ibid.
[118] Ibid p 644.
[119] *Al-Rawi v Security Service* [2011] UKSC 34. Para 145, *Dunn v Durham County Council* [2013] 1 WLR 2305
[120] *Dunn v Durham County Council [2013] 1 WLR 2305*, *Science Research Council v Nassé* [1979] QB 144, 179.
[121] *Al-Rawi v Security Service* [2011] UKSC 34 para 145.
[122] *Davis* [1993] 1 WLR 613.

may weaken the prosecution or strengthen the defence must be disclosed.[123] If any withholding of material occurs then everything must be done to protect the rights of the accused, including stopping the case in some instances.[124] PII is a powerful tool for public authorities but it is accompanied by a correspondingly strict level of oversight and safeguards from the court, in particular its exclusionary nature.

This section has aimed to outline PII as a comparator for the IPT. This is not to say that the PII is a model to which the IPT should aspire to, rather that they both face similar issues regarding disclosure and national security. Two safeguards can be drawn from PII procedures to be incorporated in the IPT. The first is the procedure surrounding disclosure of material. Where PII implements a test of strict necessity for non-disclosure of material, the IPT is more lenient. However, it is unclear how feasible the implementation of a PII test of strict necessity would be in the context of the IPT. If sensitive information was excluded from the proceedings would there be anything substantial left considering the covert nature of surveillance and the national security context the IPT operates within. A fruitful comparison may be with the incorporation of Special Advocates in Closed Material Procedure (CMP) cases.

9.6.2 Special Advocates

Although primarily used in Closed Material Procedure (CMP) cases, in a number of PII cases the possibility of appointing Special Advocates to conduct an examination of the withheld material was raised. In *Edwards* it was suggested that this would be the proper course to take in any cases where the judge must act as the tribunal of fact on an issue, such as entrapment, which might effectively determine the outcome of the case.[125] In *H* it was argued that where the accused or their representative are not present during the hearing of an application to withhold material, the decision in *Edwards* requires the appointment of a Special Advocate.[126] The House of Lords in that instance declined to institute such a rule but held that it may be necessary in exceptional circumstances to protect the interests of the accused.

Special Advocates were seen as the solution to an adverse ruling made against the UK in the ECHR case *Chahal v UK*. The case concerned the applicant's detention pending deportation

[123] *H* [2004] 2 AC 134, para 14.
[124] *H* [2004] 2 AC 134 .
[125] *Edwards v United Kingdom* (1992) 15 EHRR 417.
[126] *H* [2004] 2 AC 134.

based on the suspicion by the Home Secretary of his involvement in terrorist activities. The applicant was only able to appeal this decision to an internal Home Office advisory panel known as the 'Three Wise Men' on the basis of sensitive intelligence material. He was allowed to appear before the panel in person and call witnesses on his behalf but was not entitled to legal representation or for the sensitive material to be excluded from decision making subject to public interest immunity. It should be noted that the procedure was purely advisory and the Home Secretary was under no obligation to follow the recommendation.[127] The Home Secretary then signed an order for Chahal's deportation. The applicant then applied for judicial review of the Home Secretary's decision to deport, but the Secretary of State invoked national security considerations as grounds for the decision to deport and detain him and the court's powers of review were limited.[128] The ECtHR thus found the judicial review proceedings and the advisory panel to be in breach of Article 5(4) and 13 ECHR. Although the Court recognised that the use of confidential material may be unavoidable where national security is at stake, this does not mean that the national authorities can be free from effective control by the domestic courts "whenever they choose to assert that national security and terrorism are involved."[129] The Court then stated that there are "techniques which can be employed which both accommodate legitimate security concerns about the nature and sources of intelligence information and yet accord the individual a substantial measure of procedural fairness."[130] Specific reference was made to the Canadian "use of a security cleared counsel instructed by the court who cross-examines the witnesses and generally assists the court to test the strength of the State's case."[131]

It is unsurprising then that the UK's first preferred model of Special Advocates in the Special Immigration Appeals Commission took the form of an amicus curiae system[132] wherein the Commission would be able to appoint counsel to:

> Help it in its examination of the security evidence, and in particular to look at that evidence as if on behalf of the defendant. The Commission would then give appellants

[127] House of Commons Constitutional Affairs Committee, The Operation of the Special Immigration Appeals Commission (2004-05, HC 323-2), Ev 80, para 1.
[128] John Jackson, *The role of special advocates: Advocacy, due process and the adversarial tradition*. The International Journal of Evidence and Proof (2016), Vol 20(4) 343 – 362, 347.
[129] *Chahal v UK* 23 EHRR 413 para 131.
[130] Ibid para 141.
[131] Ibid.
[132] John Jackson, *The role of special advocates: Advocacy, due process and the adversarial tradition*. The International Journal of Evidence and Proof (2016), Vol 20(4) 343 – 362, 347.

> as full a summary as is possible in the circumstances of any evidence taken in its absence.[133]

This was envisioned to be a power with very limited usage. Introduced in 1997 in the Special Immigration Appeals Commission Act, Parliament did not anticipate its expansion in a post 9/11 national security context.[134] This is exemplified by the fact that the Government felt that the amount allocated for the legal costs of the appointed counsel should be just £1000 per year. The only substantive objection to the proposed system came from Lord Thomas of Gresford. Alluding to the principle that where a court or tribunal deals with the liberty of the subject, the subject should be told the substance of the allegation against him. Lord Thomas asked on what basis the Commission was to appoint its own counsel. Was the person appointed to take and follow the appellant's instructions and to have confidentiality and the benefit of LPP?[135] When the Bill moved to the Committee stage it was announced that the role of appointed counsel to the Commission had been reconsidered. It was here that the term 'special advocate' was first used.[136] First the power to appoint Special Advocates was moved from the SIAC to the Attorney General, in order to ensure their independence. Next, the role of the Special Advocate would be to represent the interests of the appellant in the parts of the proceedings from which he and his legal representative were excluded. Finally, the special advocate would not have a client relationship with the appellant.[137] So, then, the role imagined for the counsel shifted dramatically from amicus curiae to an independent representative for the applicant who nonetheless could not treat the applicant as a client, distinguishing the relationship significantly from regular advocacy.

Another aspect to note is the different roles Special Advocates can play in proceedings. First, there is a disclosure role, where they argue in favour of greater disclosure of closed information to the excluded party.[138] Second, there is a substantive 'representation' mode, where they advocate on the merits of the closed information against the excluded party.[139] It is the representative role wherein many of the criticisms of Special Advocates as a means to

---

[133] Lord Williams of Mostyn, HL Debs 5 June 1997, col. 736.
[134] John Jackson, *The role of special advocates: Advocacy, due process and the adversarial tradition*. The International Journal of Evidence and Proof (2016), Vol 20(4) 343 – 362, 347.
[135] Ibid p 348.
[136] Lord Williams of Mostyn, HL Debs, 23 June 1997, col. 1437.
[137] Ibid.
[138] John Jackson. (2016). The role of special advocates: Advocacy, due process and the adversarial tradition. *The International Journal of Evidence & Proof*, *20*(4), 354.
[139] House of Commons Constitutional Affairs Committee (2005) The Operation of the Special Immigration Appeals Commission (SIAC) and the Use of Special Advocates. 2004-2005 HC 323-1. 3 April.

mitigate perceived unfairness in cases involving the non-disclosure of sensitive materials.[140] If the goal of the courts is to ensure an effective adversarial process, then they are in principle less than ideal. Special Advocates can never represent the defence as well as defence advocates can.[141] Lord Kerr opined in *Al-Rawi* that because of the "inherent frailties of the special advocate system, the challenge that the special advocate can present is … of a theoretical, abstract nature only."[142] One reason for this is that Special Advocates cannot communicate with their client once they have viewed the closed material. This effectively limits them to 'taking blind shots at a hidden target'.[143] This is not to say that the Special Advocates are especially effective in their disclosure role either. A Special Advocate, Martin Chamberlain, pointed out that once the Government objects to disclosure on the grounds that it would compromise its sources, it is:

> Almost always upheld by the court. This is not because the courts neglect their function of scrutinising the objection with great care … It is simply because, without access to any independent expert evidence, they have no means of gainsaying the Government's assessment that disclosure could cause harm to the public interest. The result is that, unless the Special Advocate can point to an open source of the information in question, Government assessments about what can and what cannot be disclosed are effectively unchallengeable.[144]

It is clear that the use of Special Advocates in CMPs is less protective of the right to a fair trial than the procedure in PII, that the advocacy they implement is of a theoretical, abstract nature, and that they are no substitute for actual legal representation. However, there is a case to be made for their justification on due process grounds, as a means of ensuring a measure of procedural justice for the party excluded from the closed hearing and therefore as a legitimate human rights safeguard.[145] In *Edwards and Lewis v UK* the ECtHR held that the PII procedure used in that case did not meet the requirement to provide adversarial proceedings and equality of arms and incorporate adequate safeguards to protect the interests of the

[140] Jackson, J. (2016). The role of special advocates: Advocacy, due process and the adversarial tradition. *The International Journal of Evidence & Proof*, *20*(4), 343, 355.
[141] Ibid p 611.
[142] *Al-Rawi v Security Service* [2011] UKSC 34 para 94.
[143] *CF v Security Service* [2013] EWHC 3402 (QB), para 19, in Richard Glover, *Murphy on Evidence* (15th edn, OUP 2017) p 672.
[144] M. Chamberlain, 'Special Advocates and procedural fairness in closed proceedings' (2009) CJQ 314, p. 320
[145] John Jackson, *The role of special advocates: Advocacy, due process and the adversarial tradition*. The International Journal of Evidence and Proof (2016), Vol 20(4) 343 – 362, 347.

accused, holding that there had been a violation of Article 6. Within this case the Court also noted the use of special counsel as part of relevant domestic law and practice, citing extensively the Auld Report which recommended the introduction of Special Advocates.[146] In *H*, Lord Bingham held that:

> None of these problems should deter the court from appointing special counsel where the interests of justice are shown to require it. But the need must be shown. Such an appointment will always be exceptional, never automatic, a course of last and never first resort. It should not be ordered unless and until the trial judge is satisfied that no other course will adequately meet the overruling requirement of fairness to the defendant.[147]

The use of Special Advocates can then be seen as the adaptation of the adversarial tradition in order to bring a greater measure of procedural fairness to the proceedings.[148] It can be argued that Special Advocates in their disclosure role are more akin to advocates of the court or amicus curiae.[149] A 2009 Justice report argued that, just as the prosecution or government counsel represents the public interest in non-disclosure, the 'public interest advocate', as it refers to Special Advocates in this role, represents the public interest in disclosure.[150] In their view, there is nothing to be gained by confusing an advocate who argues for disclosure in a PII claim with an advocate who helps determine the substantive facts in issue in a secret trial. In Justice's view, there is considerable benefit to using these public interest advocates in other *ex parte* applications such as search warrants, and surveillance warrants.[151]

A useful example of how these public interest advocates may operate is the Queensland Public Interest Monitor under the Police Powers and Responsibilities Act 1997. Under this Act the Monitor both supervises police compliance with applications for search and surveillance warrants and appears at any hearing of an application for a surveillance warrant or covert search warrant in order to test the validity of the application. Because police applications for these warrants are made *ex parte* without the defendant's knowledge, the Monitor aims to introduce an element of adversarial proceedings into what is otherwise a

[146] *Edwards and Lewis v. UK* (2005) 40 EHRR 24, para 44.
[147] *H* [2004] 2 AC 134 para 22.
[148] John Jackson, *The role of special advocates: Advocacy, due process and the adversarial tradition*. The International Journal of Evidence and Proof (2016), Vol 20(4) 343 – 362, 355.
[149] Ibid.
[150] Justice (2009) Secret Evidence. London: Justice.
[151] Ibid para 445(a).

one-sided process.[152] This is done by presenting questions for the applicant to answer, examining and cross-examining any witness, and making submissions on the appropriateness of the application. It should be noted however that the Monitor's task is not to represent the interests of the absent party, but the public interest more generally.[153] This may make it more akin to amicus curiae than Special Advocates.

As discussed earlier, cases requiring a Special Advocate are rare, even within the IPT's jurisprudence. It would not be the first resort as even in SIA cases the IPT may push for concessions and other ways around the disclosure of sensitive material before resorting to closed hearings and the appointment of a Special Advocate. Finally, in such a case where the IPT intends to hold a closed hearing, the appointment of a Special Advocate is a means of mitigating the perceived unfairness of the closed session. While Special Advocates are not a panacea to this problem, especially when compared to allowing the complainant and their legal representation to participate fully in the hearing, it is surely better than the sheer lack of participation under the current system. The IPT has appointed Special Advocates in the past, but they act more as 'amicus curiae' meaning they may assist the Tribunal rather than the complainant.[154] Thus they have no requirement to be partisan.[155] Lord Anderson in his review of the Investigatory Powers Act highlighted that Special Advocates could be utilised by the IPT but declined to make a firm recommendation on the issue either way as there was strong disagreement as to the effectiveness of counsel as amicus curiae versus Special Advocates.[156] He based this lack of recommendation on two issues. First it can be argued that the nature of IPT cases reduces the need for an advocate to be able to take instructions on behalf of a claimant. Second, the belief that counsel to the Tribunal, or amicus curiae, is capable of having more influence in IPT closed proceedings than would be attainable by a Special Advocate.[157]

The question of amicus curiae versus Special Advocates may initially seem to hinder this section's recommendation of the adoption of Special Advocates into IPT proceedings. However, this tension can be resolved via returning to the original formulation of Special

[152] Ibid para 333.
[153] Report of the Public Interest Monitor, October 2006, para 8.
[154] *Big Brother Watch* para 142.
[155] Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129 p 136.
[156] D. Anderson, 'A Question of trust, Report of the Investigatory Powers Review' para 14. 108.
[157] Ibid.

Advocates by the Parliament in 1997. While the initial description of the role of special counsel was effectively amicus curiae, as it was appointed by the Commission in question in order to help it examine the closed material "as if on behalf of the applicant",[158] this was rejected in favour of a system where the Special Advocate was appointed by the Attorney General and its role was to represent the applicant and their representation in closed proceedings, while still not having a client relationship with the advocate. The key distinguishing characteristics are then the independence of the advocate from the judicial body in question, and their perceived role. This is significantly more effective in term of procedural justice to the applicant.

Given that while the Special Advocate and the amicus curiae may have substantially the same effect on the IPT's decision to disclose, the impact on the procedural justice of the applicant is substantial. Consider how an applicant may perceive their likelihood of being treated fairly in a closed proceeding based on the Tribunal appointing counsel who is obliged to serve itself rather than the applicant. Compare this with how an applicant may perceive this same likelihood with an independently appointed Special Advocate. In both, their participation is limited by the closed proceedings but while the Special Advocate may not consult with the applicant after viewing the closed material, they are allowed to confer prior to this, and the applicant may inform the advocate of the arguments they wish to make on what they perceive the closed material is likely to be. In terms of neutrality, the applicant is likely to perceive the IPT as favouring the Government on questions of disclosure of sensitive information, considering the outcome of the *Steiner* case discussed above and the IPT's statutory commitment to not disclosing anything that may have national security implications. This perception would further weaken their belief in the ability of amicus curiae to make arguments on their behalf. In terms of respect, the applicant cannot be certain that their arguments were seriously considered by the Court in a closed proceeding as they have no way of knowing if the Tribunal appointed amicus curiae for them and how said counsel acted. With a special advocate, the applicant can be reassured beforehand that their counsel will represent them as fully as possible, with the caveat that they will have to take this on faith. Finally, the applicant is more likely to trust in the decision of the court to disclose or not if they know that there was an independently appointed counsel whose sole purpose was to represent them.

[158] Lord Williams of Mostyn, HL Debs 5 June 1997, col. 736.

As Chamberlain alluded to earlier, the likelihood of such a Special Advocate succeeding substantively may be small,[159] but the due process and sense of procedural fairness provided to the applicant in these proceedings would be significant. Returning to the cases examined earlier, *Belhadj* and *Steiner*, without altering the substantive outcomes of either of these cases it can be seen how the use of a Special Advocate would improve the applicant's perception of the procedural justice the IPT afforded them. In *Belhadj*, while the Tribunal sided with the applicants on the larger question of law as to what a 'no determination' outcome means, and disclosed material accordingly, it disclosed a relatively tiny amount of material following a closed hearing on the matter. Of the nine applicants, and associated material, the Tribunal disclosed two documents concerning one claimant. Without any representation in said closed proceedings, the applicants were likely to feel that they were lucky to receive any disclosure at all and had only a slight chance of convincing the Tribunal otherwise. If they knew that they had a Special Advocate pushing for more disclosure of material, they would be more likely to feel they had been given a fair shot and that whatever security concerns the Government had were legitimate. Likewise, the lack of procedural justice in *Steiner* could have been alleviated by appointing Steiner a Special Advocate. It would be easier to convince the applicant of the Government's need to keep material on a deceased spy closed if he knew that someone representing him had seen said material and argued his case accordingly.

There is the danger that the use of Special Advocates in this manner may simply be a way for the IPT to legitimate its rulings without actually affording any more procedural justice to the applicant. This is similar to the process danger invoked about the use of Special Advocates in Parole Boards, where it will be easier to withhold information from a prisoner if there is a scheme that does something to help out the prisoner when said information is withheld.[160] Special Advocates may be a means of mitigating the potential unfairness of closed proceedings, but this "mitigation may have the unintended effect of managing, legitimising and normalising the use of closed proceedings".[161] If Chamberlain's argument that the courts always uphold the objection of the Government to disclosure due to lack of expertise holds, then the procedural justice provided the Special Advocates would seem to be illusory. However, the specialised nature of the IPT alleviates this somewhat as, to a certain extent, it has the relevant expertise to gainsay the value and sensitivity of closed material. While it may

[159] M. Chamberlain, 'Special Advocates and procedural fairness in closed proceedings' (2009) CJQ 314, p. 320
[160] Tim Endicott Administrative law (4th edn) 2018 OUP P 156.
[161] Aileen Kavanagh "CASES: Special Advocates, Control Orders and the Right to a Fair Trial." (2010) 73 Modern Law Review 836

still defer to the executive on national security grounds, it has the expertise to at least challenge the executive's weaker cases for non-disclosure.

The IPT finds its most direct comparator in the Closed Material Procedures mechanism. While Special Advocates are a flawed means of mitigating the procedural unfairness of closed sessions, they could be reasonably implemented into the IPT's proceedings for the purpose of increased procedural justice to the Tribunal's applicants. The fact that the IPT's proceedings surrounding disclosure of material and overall fairness could so reasonably be improved, undermines the argument for its overall effectiveness and adequacy as a safeguard for the surveillance regime under the IPA. However, this claim is tempered by the fact that the ECtHR has found the IPT to be capable of operating as an effective safeguard in *Kennedy*[162] and *Big Brother Watch*.[163]

9.7 Does the IPT Meet Human Rights Requirements?

The ECtHR has addressed the question of the IPT as an effective domestic remedy in both *Kennedy* and *Big Brother Watch*.[164] In *Kennedy* the Court took issue with the fact that the IPT had no power to annul any of the RIPA provisions or find any interception arising under RIPA to be unlawful as a result of the incompatibility of the provisions themselves with the Convention.[165] The Court took note of the extensive powers of the IPT to investigate complaints before it and to access confidential information, but did not see clearly their relevance to a legal complaint regarding the operation of a legislative regime. The Court also noted that the IPT is not able to disclose information to an extent, or manner, contrary to the public interest or prejudicial to national security. Thus, the IPT did not meet the requirements of an effective domestic remedy. However, in *Big Brother Watch* the Court accepted the UK government's argument that the jurisprudence of the IPT that the post *Kennedy* IPT jurisprudence showed that it could offer an effective remedy which could have been pursued by the applicants. The GC in *Big Brother Watch* examined the IPT as a form of ex post facto review. In this evaluation, the GC highlighted the ability of the IPT to award compensation, quash or cancel warrants and to require the destruction of records. The GC also highlighted how the IPT's legal rulings were published on its own dedicated website "thereby enhancing

[162] *Kennedy v United Kingdom* (2011) 52 EHRR 4 para 184.
[163] *Big Brother Watch and Others v. The United Kingdom,* App nos. 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018), para 318.
[164] See chapter 4 on 'Bulk Interception Caselaw of the ECHR'
[165] *Kennedy v. UK* (2011) 52 EHRR 4 para 109.

the level of scrutiny afforded to secret surveillance activities in the United Kingdom".[166] In the view of the GC the IPT provided a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services.[167] Thus, the IPT is likely to continue be considered an effective domestic remedy going forward. However, as this chapter has shown, this does not mean it is capable of protecting against the harms caused by bulk interception in the sense that the lack of substantive and procedural justice available to applicants.

9.8 Conclusion

This chapter has examined the review and oversight mechanisms present in the IPA regime; namely the auditing and inspections conducted by the Investigatory Powers Commissioners Office (IPCO), the annual reporting done by the IPCO, and the Investigatory Powers Tribunal (IPT). It is clear from the first part of this chapter that the auditing and inspection carried out by the IPCO is thorough. However, the limits of transparency in this context hampers the ability of the IPCO to protect against the harms of bulk surveillance powers. As evidenced by the example of Nigel Lang there is also the issue with the impact of errors in a bulk surveillance context which undermines the level of protection provided by the auditing and reporting functions of the IPC. The effectiveness of the IPC as a safeguard is weakened further by the structural and institutional problems of independence highlighted in the previous chapter. The proximity of the IPC to the executive, as well as the fact that the IPC is responsible for both the issuing of warrants and the reporting of errors creates at least the appearance of a conflict of interest.

The second part of the chapter focused on the effectiveness of the IPT as a domestic remedy. Due to the sensitive nature of the material the IPT examines, there is a lack of transparency surrounding its rulings which makes evaluating its effectiveness as a safeguard based on substantial outcomes difficult. While there were observable trends in the reporting of case results by the IPT these are too easily explained away without any further detail provided in the Tribunal's reporting. Still, the fact that just 31 of 1408 complaints were found in favour, with the majority being ruled as frivolous or vexatious (661/1408) or receiving no

[166] *Big Brother Watch GC* para 412
[167] Ibid para 413

determination (459/1408), is noteworthy in itself as it implies that applying to the Tribunal is rarely successful.

In light of this, this chapter focused on the procedural justice afforded to applicants by the IPT. This was done through the application of Brems and Lavrysen's criteria for procedural justice in human rights adjudication to the IPT's case law, focusing on participation, neutrality, trust and respect. This found that while the procedural justice provided by the Tribunal in cases of overt surveillance by the police or local councils was plentiful, it shrunk as the analysis encountered cases concerning the activities of SIAs and national security. The cases of *Paton*, *Belhadj*, and *Steiner* were used as case studies to illustrate this decline.

This led to a comparison with other measures which deal with sensitive material: Public Interest Immunity and Special Advocates. In PII the IPT found an unfavourable comparator, one which better seeks to ensure equality of arms through the exclusion of sensitive material which the Government wishes to keep from the case proceedings altogether. However, it is not clear whether it is feasible to implement a PII approach in the IPT context. Additionally, in terms of procedural justice, such an act may cause an applicant to perceive the IPT as more neutral and in turn trust in its decision more. However, it does nothing to increase the participation of the applicant, nor does it make them feel more respected by the Tribunal's proceedings. Nonetheless, this section argued that a form of the Special Advocate used in PII and CMPs could be implemented in the IPT's proceedings. Acting in its less controversial disclosure role, a Special Advocate could improve the procedural justice afforded to the applicant in closed proceedings along all four of Brems and Lavrysen's criteria. This was demonstrated through a return to the IPT cases of *Belhadj*, and *Steiner*, to show how the procedural justice perceived by the applicants could be improved without altering the substantive justice given out by the Tribunal. In conclusion, the IPT is a flawed safeguard in terms of the procedural justice it metes out. While it would be very difficult to alter the substantive justice, it is relatively simple to increase the procedural justice through the implementation of a Special Advocate system.

Overall, the faults of the IPT speak to a further need for reform. While the IPT has undoubtably improved over the course of its twenty-one-year lifespan, this chapter has shown that there are further reforms which could be made to maximise its efficacy as a domestic remedy for those who believe that they have been subject to the use of surveillance powers. While the IPT is likely to continue to be held as an effective domestic remedy by the ECtHR

its lack of substantive and procedural justice to its applicants prevents it from protecting against the harms of bulk surveillance as effectively as it could.

10. Conclusion

This thesis set out to explore the issues stemming from the use of bulk surveillance powers in the UK. These powers have been identified as broad, with far-reaching capabilities which cause harm to individuals in qualitatively different ways. This thesis has also examined the level of protection European human rights law can have against the harms caused by the use of these powers. Given the relative recency of the Investigatory Powers Act 2016 and the fact that neither the ECtHR nor CJEU has addressed said Act, this thesis sought to answer two questions:

1. Are the bulk surveillance powers contained within the Investigatory Powers Act compatible with European Human Rights Law?
2. Is the level of protection provided by European Human Rights Law capable of protecting against the harms of bulk surveillance?

This chapter first presents the findings of this thesis before discussing both the theoretical and policy implications of these findings. This is followed by a discussion of the limitations of this study alongside directions for future research.

10.1 Findings

This thesis outlines the breadth of the powers under the Investigatory Powers Act 2016. In order to offset this broadness, the IPA provides a series of safeguards. The primary ex ante safeguard is a system of authorisation by the Secretary of State with approval from a JC called the 'double-lock' system. In terms of ex post facto review, the IPA contains the Investigatory Powers Tribunal and the Annual report by the Investigatory Powers Commissioner. Finally, in terms of examination safeguards, the IPA contains operational purposes which are in effect a narrowing of statutory purposes to something more specific and limiting. These are set out in the warrant and decided at the authorisation stage. While the authorisation and review stages of the bulk surveillance process have their own supervision, the selection for examination stage is set out in the authorisation stage and reviewed in the ex post facto stage with no ongoing supervision.

This thesis has also set out the harms provided by bulk interception showing how the technology and application of bulk interception under the IPA makes it possible for a huge amount of data to be collected, filtered and examined in order to make clear, intrusive profiles of individuals' behaviour and identities which can be aggregated into large searchable databases. The harms stemming from this go beyond just privacy harms to the individual. Rather these harms to privacy, freedom of expression and freedom of assembly go beyond the

individual towards societal harms in the form of the chilling effect the knowledge of the bulk interception regime causes. This chilling effect can be most felt in the harms to freedom of expression and freedom of assembly, the knowledge of the ability of the state to monitor your communications in a political climate where the right to effective protest is being curtailed and there is an increasing emphasis on regulating online speech is going to have a large impact on a given individual's desire to exercise their rights. The distinction made between the intrusiveness of content versus metadata obscures the reality of bulk surveillance. A clearer distinction to draw would be between the varying types of metadata: application, network and service use level data. While network level data is relatively non-intrusive, application and service use data are. Chapter 5 furthered this analysis demonstrating how the different powers of bulk interception, acquisition, and equipment interference are qualitatively different to each other. This holds for their intrusiveness, their ability to break encryption, the expectation of privacy they are associated with, and their usefulness to the intelligence community. This has a number of implications for the safeguarding of bulk surveillance powers under the UK regime.

Closer examination of the so-called double-lock system, in chapter 8, revealed that the protection offered by this safeguard comes down to the level of deference the JCs afford to the executive. While it is difficult to see what level of deference a JC will afford the executive due to the covert nature of surveillance, several institutional factors are likely to influence it in a problematic fashion. The most significant of these is the lack of independence from the executive. This is compounded by the ability of the Secretary of State to appeal the decision of a JC to the Investigatory Powers Commissioner. Another factor which may affect the level of deference is the lack of inter partes conflict in the authorisation system.

Following on from this chapter 9 examined the ex post facto review safeguards present, namely the Investigatory Powers Tribunal (IPT) and the annual reporting by the Investigatory Powers Commissioner's Office. In terms of the IPT acting as a domestic remedy, it was found to be lacking in both substantive and procedural justice. The issue of executive influence on the Tribunal was also raised as the Secretary of State can set the rules for it. The annual reporting by the IPC is also flawed in that the IPC is also involved in the authorisation of warrants. This creates at least the appearance of a conflict of interest as the aim of the reporting is to address possible errors in the authorisation and operation of the surveillance powers. Therefore, this thesis argues that given the nature and operation of the broad powers granted by the IPA the safeguards provided for in the legislation are not sufficient to protect against the potential harms.

This thesis has also examined the level of protection provided by European Human Rights Law and whether this is capable of protecting against the harms of bulk surveillance. First, in chapter 3, it was found that regarding the application of Article 8(1) in the context of targeted surveillance the Court hasn't addressed certain key questions in a social media context such as: the expectation of privacy on different platforms, the aggregation of publicly available social media data, and whether membership of an online community constitutes membership of a proscribed group. In terms of Article 8(2) the chapter showed the tension between the Court's desire to provide meaningful protection and its subsidiary role in the context of national security. This tension has led the Court to provide states with a wide margin of appreciation in how they choose to operate surveillance regimes.

Next this thesis considered the ECtHR's caselaw on bulk interception where the employment of a wide margin of appreciation led the ECtHR to overreliance on a set of foreseeability requirements known as the minimum safeguards against abuse test (or the *Weber* requirements). Here it was confirmed that the decision to operate a bulk surveillance regime is within the state's margin of appreciation, providing that they meet these minimum safeguards. In the GC judgments of *Big Brother Watch* and *Centrum* this test was updated to the "end-to-end safeguards" test which added requirements of independent authorisation, supervision and ex post facto review to the minimum safeguards. Despite the Court stating that interference is at its highest at the selection for examination stage, this is not reflected in the end-to-end safeguard test.

This analysis was complemented by the analysis of the CJEU's caselaw on data retention. While this initially appeared to be a stronger source of human rights protection against the dangers of bulk surveillance than the ECHR, in reality the CJEU has provided another set of safeguards by which to test the compatibility of bulk surveillance. However, these safeguards are narrower in application than the ECtHR's. While the ECtHR has only addressed bulk interception thus far, the *Big Brother Watch* safeguards can be applied to the other bulk powers, even if these safeguards do not adequately reflect the realities of these other powers. The CJEU safeguards can only be applied to powers which require electronic communications providers to retain data, and those which require electronic communications providers to provide access or transmission of data. Thus, while it applies to bulk acquisition under the IPA it does not necessarily apply to bulk interception, bulk equipment interference or bulk personal datasets. Next there is the issue that the CJEU safeguards are in effect quite similar to the ECHR safeguards. It isn't clear that the protection provided by these safeguards is higher than the safeguards under *Big Brother Watch*. Finally, while the CJEU does not explicitly invoke a margin of appreciation for a member state's decision to utilise bulk

surveillance for national security purposes. The rulings in *Privacy International* and *La Quadrature* make clear that in the national security context the CJEU views the operation of regimes which may be wider in scope than bulk surveillance are, in principle, permitted. As bulk surveillance operates only within the national security context, it again isn't clear that the CJEU caselaw can provide much more protection than the ECtHR's against the harms of bulk surveillance.

This thesis' key findings can be summarised as follows. The Investigatory Powers Act 2016 grants the executive broad, invasive powers which are qualitatively different from each other in terms of both operation and harms. The safeguards provided for the use of these powers by the IPA are flawed and unable to protect against the harms incurred by the use of bulk surveillance powers. Yet the IPA is simultaneously likely compliant with existing European human rights law. These findings present both theoretical and policy implications.

10.2 Theoretical Implications

10.2.1 Clarifying Bulk Surveillance in the UK Context

This thesis makes a contribution to the existing literature by clarifying the operation of bulk surveillance within the UK context. Academic literature on the operation of bulk powers to date have focused primarily on examining the use of these powers in the UK context and in particular, the NSA.[997] Less attention has been paid to the reality of the operation of bulk surveillance within the UK context and, in particular, the use of bulk powers by GCHQ. Chapter 3 uses a mix of official sources, derived from UK official documents and unofficial sources, derived from the Snowden leaks in order to paint a clearer picture of the operation of bulk interception under the IPA and the multivariate harms caused by the existence and operation of such a system on an environmental level. This points towards a wider conclusion that human rights jurisprudence and analysis should move from individual harms towards societal harms as even if the safeguards present within these regimes are able to contain the use of these broad powers, the chilling effect they may have on society is where the real harm may be realised. Chapter 4 clarifies this finding by outlining how exactly each of the four bulk powers of interception, acquisition, equipment interference, and personal datasets fundamentally differ from each other. This implies a need for further study on the harms

[997] Michelle Cayford, Coen Van Gulijk and Pieter Van Gelder, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014), Lonneke Van der Velden, 'Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance' (2015) 13 Surveillance & Society 182, Michelle Cayford and Wolter Pieters, 'The effectiveness of surveillance technology: What intelligence officials are saying ' 34 The Information Society 88, Michelle Cayford, Wolter Pieters and Constant Hijzen, 'Plots, murders, and money: oversight bodies evaluating the effectiveness of surveillance technology' 33 Intelligence and national security 999.

stemming from the operation of these systems and how they may be properly limited as currently the safeguarding approach based on bulk interception leaves significant gaps wherein these powers can be utilised to bypass restrictions, such as the use of bulk acquisition within the UK rather than limited to the foreign focus safeguard.

10.2.2 Shifting the focus to the Adequacy of Safeguarding in European Human Rights Law

Literature on the surveillance law principles of the ECtHR has focused on the wide margin of appreciation which arguably undermines the important role played by the ECtHR in protecting individual rights.[998] Yourow takes a similar line in regard to the margin of appreciation doctrine in general, stating that the Court is always prepared to approve rights restrictive state action as falling within the wide margin of appreciation states enjoy as aspect of sovereignty in the national security context.[999] This appears to be in conflict with the Court varying the size of the margin of appreciation it affords states on a case by case basis. In contrast to this trend, this thesis shifts the discussion from the question of whether these powers should be within a contracting party's margin of appreciation towards a systematic analysis of the safeguards these parties use to, arguably, keep these powers to what would be considered proportionate to their legitimate aims of national security.

10.2.3 Systematic Critique of the Double-Lock system

The works of Scott[1000] and Woods[1001] have focused on the extent to which the judicial commissioners and the wider double-lock warrant authorisation blur the lines between regulatory and judicial oversight, however each stops short of a systematic critique of how the JCs are likely to operate under this system. At the same time discussions on the double-lock and the IPC fit into wider academic literature on the appropriate deference in judicial review in a national security context. The implications of the critique of the Double-lock system present in this thesis are thus two-fold. First this chapter attempted to push discussion about the effectiveness of this safeguard away from questions of the standard of review or the appropriate deference which a JC should show the executive when approving a warrant. Rather the JCs will likely take a contextual approach to each warrant which is imperceptible from an outside perspective. As the approach of the JCs is imperceptible it is more productive

[998] Kirsty Hughes, 'Mass surveillance and the European Court of Human Rights' (2018) 6 EHRLR 589
[999] Howard Charles Yourow *The margin of appreciation doctrine in the dynamics of European human rights jurisprudence* (Martinus Nijhoff Publishers 1996). p. 107
[1000] Paul F Scott, 'Hybrid institutions in the national security constitution: the case of the Commissioners.' 39 Legal Studies 432
[1001] Lorna Woods, Lawrence McNamara, Judith Townend, 'Executive Accountability and National Security' (2021) 84 Modern Law Review 553, Lorna Woods, 'The Investigatory Powers Act 2016' (2017) 3 Eur Data Prot L Rev 13.

to push for reform of visible inadequacies with the IPC. In line with this chapter 8 highlighted a number of structural and institutional factors which may impact a judicial commissioner's ability to provide effective oversight to the use of bulk surveillance powers which include the lack of *inter partes* argument, the proximity of the IPC to the executive and the appointment procedures of the IPC.

10.2.4 Procedural Justice Analysis of the IPT

This thesis adds to the extensive criticism of the IPT, in particular Wilson's work on the lack of fairness in the IPT's procedure, with a procedural justice analysis of the IPT's caselaw.[1002] This was done through the application of Brems and Lavrysen's criteria for procedural justice in human rights adjudication to the IPT's case law, focusing on participation, neutrality, trust and respect.[1003] This found that while the procedural justice provided by the Tribunal in cases of overt surveillance by the police or local councils was plentiful, it shrunk as the analysis encountered cases concerning the activities of SIAs and national security. This thesis also compared the procedures of the IPT with that of PII and special advocates to show how the procedural justice perceived by applicants could be improved without altering the substantive justice given out by the Tribunal through the relatively simple implementation of a special advocate system.

10.3 Policy Implications

10.3.1 Need for new approach from the ECHR/CJEU

As of the Grand Chamber judgments of *Big Brother Watch* and *Centrum*, in order to minimise the risk of these bulk powers being abused the Court considered that the process must be subject to "end-to-end safeguards". This is specifically described as meaning that, at the domestic level, "an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken."[1004] However, this was immediately qualified as consisting of, at least in the case of bulk interception, independent authorisation at the outset and, supervision and ex post facto review.[1005]

This qualification is an error on the Court's part. In order to for an assessment to be made at each stage of the process of the use of a bulk power, an assessment of the necessity and

[1002] Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129
[1003] Eva Brems and Laurens Lavrysen. "Procedural justice in human rights adjudication: The European Court of Human Rights." *Human Rights Quarterly* (2013): 180.
[1004] Ibid para 350.
[1005] See the discussion of the Grand Chamber judgment of *Big Brother Watch* in Chapter 3.

proportionality must be made at the selection for examination stage as well. If the evaluation of Y's case is limited to the robustness of the IPT as a domestic remedy and the supervision and authorisation of the warrant provided by the IPC and the double-lock process, then the

Throughout this thesis emphasis has been placed on the minimum safeguards against abuse test in the Court's approach to bulk surveillance. As mentioned above the Court has very recently developed this into a 'end to end' safeguard approach. This is part of the greater acknowledgment by the Court that it is necessary to update their approach in order to better reflect the realities of contemporary bulk surveillance. However, as detailed above this updated approach does not encompass examination safeguards and thus does not adequately reflect how these bulk surveillance powers operate.

The solution to this is relatively simple as it requires the acknowledgment of the selection for examination stage as a distinct part of the surveillance process. Owing to the margin of appreciation in this national security context these examination safeguards will be minimum safeguards. Requirement four of the *Weber* requirements mentions the procedure behind examination as a foreseeability requirement, however this is not sufficient.[1006] What is needed is an independent assessment of the proportionality of examination following acquisition or collection. Only then can the independent authorisers of these warrants make a clear and accurate evaluation of the intrusion this examination will cause on affected individuals. This is doubly true when considering aggregation of data from multiple bulk warrants.

It is essential that within the selection for examination stage there be separate safeguards for the examination of the acquired material, and for the aggregation of the acquired material. There are instances wherein it is proportionate to examine acquired material but not proportionate to aggregate it. If the Court's approach is to align with the Court's concerns about the dangers of aggregation, then the minimum safeguards test should be updated to reflect this.

10.3.2 The Need for Examination Safeguards in the IPA

This all points to a need for a renewed focus on examination safeguards in the UK legislation. The focus on flawed ex post and ex ante safeguards in the UK legislative framework to offset this lack of effective examination safeguards is insufficient in the context of bulk interception. This limitation is more problematic in the context of the other bulk powers such as bulk acquisition.

[1006] *Weber and Saravia v. Germany* App no. 54934/00 (ECHR, 29 June 2006) para 95.

In bulk acquisition the limitation to only examine in accordance with the operational purposes of the warrant does not effectively limit the scope of examination. The ability for SIAs to take the data from multiple bulk warrants and aggregate them is where the real intrusion into privacy begins. Once in the aggregated database, previously free-floating pieces of service use metadata and subscriber information may be constructed into comprehensive data profiles of identifiable individuals. Profiles can be retained for as long as there is at least one ground for which they may be necessary, or likely to become necessary, to retain them.

In the IPA context this points to a need for further oversight and authorisation at the selection for examination stage. Currently, the sole examination safeguard is set out in the ex-ante stage, as part of the double-lock authorisation process. The issue with this is that it cannot account for the data which will be collected under the warrant or what might be revealed if said data is combined with data from other warrants.

One possible solution to this problem is the implementation of a secondary warrant system for the aggregation of data. If, upon acquiring the communications data from a CSP, the SIA who initially applied for the warrant wished to aggregate the data with those collected from other bulk warrants, they would have to apply for a warrant to do so. The format of these warrants could follow from the bulk acquisition warrant; detailing the sources of the data, the aim of the aggregation, the necessity and proportionality of the aggregation, the duration that this data could be aggregated for, any protected data which would be subject to aggregation. Owing to the potentially intrusive nature of such a searchable database, warrants to issue such aggregation should be subject to correspondingly strict scrutiny. Duration should be limited to six months and renewal should be subject to strict necessity. Once the six-month period of the warrant had elapsed the data should be immediately disaggregated, and the profiles created as a result of it should be immediately deleted if they are not necessary for an ongoing operation.

10.3.3 Equate content and communications data as the same level of interference

While this is never explicitly stated within the IPA a foreign focus safeguard is omitted in the bulk acquisition power which is present in both the bulk interception power,[1007] and the bulk equipment interference power.[1008] In the bulk interception power both content and communications data is subject to this safeguard, in bulk equipment interference communications (content and related communications data), and equipment data are subject to this safeguard. Bulk acquisition is exempt from this safeguard, and bulk acquisition is solely concerned with communications data. This implies that the restriction to

[1007] IPA s 136 (2)(a-b).
[1008] IPA s 176 (1).

communications data justifies its use on individuals known to be within the UK. Another justification for this is that it reflects the nature of the bulk acquisition power as an intelligence gathering capability.[1009]

This underestimation of the identifying quality of communications data is a fundamental issue with the bulk acquisition power. The ability for SIAs to use bulk acquisition nationally is predicated on the fact that it does not acquire content data, only communications data. This presumes that communications data is not as intrusive as content. However, this is inaccurate. Communications data is too broad a term to accurately define what can be gained through the use of bulk acquisition. It is easier to utilise the terminology discussed in chapter 3, of application level, network level, and service use metadata. While network level metadata is first used to answer the question who speaks with whom, application level metadata "can directly reveal sensitive information such as political, religious or philosophical opinions or beliefs, as well as information concerning health or sex life."[1010] Service use metadata stored by web or application servers can mirror both network and application level data. While bulk acquisition is presented as simply being concerned with communications data (more specifically network level metadata) in reality it is most likely concerned with service use metadata. This points to the issue with communications data used as a dichotomous term with content, when the reality is more complex. The data which bulk acquisition uses can be more revealing than content data. This would be contrary to the justification for bulk acquisition not requiring a foreign focus.

If these levels were applied to the bulk acquisition power and if the bulk acquisition warrant was only concerned with the collection of network level metadata then all that would be collected are the IP addresses of the group members. The details would have been captured when the group members communicated with the server. Restriction to network level metadata would exclude email addresses, details contained with the profile such as age and address, phone numbers as well as device details. Given that a list of IP addresses alone does not reveal much about an individual's identity, restriction to network level metadata would likely limit the effectiveness of bulk acquisition as an intelligence gathering capacity. The use of this three-level classification of data would solve this issue. A bulk warrant which was limited to this network level meets the lowered level of intrusion promised by the bulk acquisition warrant and therefore not be subject to the foreign focus safeguard. A bulk warrant

[1009] Bulk Acquisition code of practice para 3.5.

[1010] Sophie Stalla-Bourdillon, Evangelia Papadaki, and Tim Chown. "Metadata, traffic data, communications data, service use information… What is the difference? Does the difference matter? An interdisciplinary view from the UK." In *Data Protection on the Move*, pp. 437-463. Springer, Dordrecht, 2016. P1.

which wishes to acquire data from the application or service use level is as intrusive as one which aims at collecting content and thus should be subject to the same safeguards.

The application of principles developed through the consideration of offline scenarios to cases involving social media platforms presents a number of issues both for the ECHR or CJEU's approach[1011]and for the protection against the harms of bulk surveillance in general. One such issue concerns equating membership of a proscribed organisation with engagement with online groups.

A given warrant may have the operational purpose to acquire the data of online groups associated with the proscribed group National Action. However, this does not mean that the groups are run by National Action. A Telegram channel may be titled "Far-Right Memes" and have a dominant culture or set of users who post National Action propaganda or be fully fledged members of the proscribed group. However, this does not mean that by joining said channel an individual is joining National Action. A large number of the channel's users may be proponents or members of other far right nationalist groups which seek power through electoral means, or just individuals with far-right political leanings. Phadke & Mitra conceptualise these as different roles which users can take in an extremist movement: solicitors, flamers, educators, motivators and sympathisers. This framework places solicitors, accounts which solicit participation and funding for the movement, as the most involved and sympathisers as the least. A sympathiser is an account which is a fringe supporter of the extremist movement who sparingly engages with links from the extremist websites.[1012] However, all are treated as though they are potential members of this proscribed group when their communications data is acquired. This is also a concern for researchers studying these groups, as they may be subjecting themselves to the use of these bulk surveillance powers in the course of their work.

10.3.4 Account for the specific qualities of social media

Another issue concerns the right to be forgotten or, in the case of social media, the right to delete. Continuing with the example of a warrant with the operational purpose to acquire the data of online groups associated with the proscribed group National Action. Users captured in the six months of a given warrant's duration may choose to cease their involvement with the extremist group, perhaps through the use of de-radicalisation programmes. However due to

[1011] See Chapter 2 on the application of ECHR Article 8 jurisprudence to social media.
[1012] Shruti Phadke and Tanushree Mitra. (2021). Educators, Solicitors, Flamers, Motivators, Sympathizers: Characterizing Roles in Online Extremist Movements. *arXiv preprint arXiv:2105.08827*.

the wide nature of the necessity test for retention their data will be retained long after they cease to be a threat. This points to a larger problem with the deletion of content and data.[1013]

Given the potential length of retention of these datasets, profiles on these individuals may exist long after it is necessary to do so. These users may delete these social media profiles but still be listed in a far-right extremist database. The Court has stressed how information about an event which was initially public becomes a part of a person's private life as it "recedes into the past".[1014] In *Segerstedt-Wiberg* the Court held that the retention of data for 30 years was too long but did not rule on what an appropriate length of time for retention would be. Given the volume and intrusiveness of the data collected by modern bulk surveillance techniques an appropriate period would likely be far shorter than 30 years. This may point to a consideration for data which has been deleted to be removed from retained datasets. However, this should be balanced against the tendency for extremist groups and users to be banned and deleted by the social media platforms themselves. The IPT may be the appropriate remedy for this issue as an individual who believes themselves to be subject to bulk acquisition may apply to it. If the individual finds that his data has been retained, he should be able to request that it be deleted as he has deleted the data himself. In granting this request the Tribunal should consider the national security implications of doing so.

The final issue concerns the expectation of privacy online. A given individual in the above example may have their data collected from three different groups: a public Facebook group, a public WhatsApp group, and a private Telegram channel. Each of these has a different expectation of privacy. Being a member of a public Facebook group conveys a low expectation of privacy as members know that their posts and membership of the group are open for all to see. A WhatsApp group, while public exists on a platform which is known for its peer-to-peer encryption on messages. WhatsApp advertises itself as a platform which puts their users' privacy first, thus members will have a higher expectation of privacy than Facebook users. Finally, an invite only Telegram channel is predicated on secrecy. In social media intelligence operations (SOCMINT) data is considered open if it is freely accessible to all that wish to access it, whereas closed data is restricted by Friends locks, passwords, encryption, invite requirement etc.[1015] Using the SOCMINT classification for open and closed data sources the Facebook and WhatsApp groups can reasonably be considered open as neither require a password nor invite to access. Whereas the Telegram channel requires an

[1013] See Chapter 2 on the Right to be Forgotten p.
[1014] *MM v United Kingdom* para 188, *Rotaru v Romania* paras 44 – 45.
[1015] Lillian Edwards and Lachlan Urquhart (2016). Privacy in public spaces: what expectations of privacy do we have in social media intelligence?. *International Journal of Law and Information Technology*, *24*(3), 279-310.

invitation to access. Telegram is a social media platform which utilises encrypted one-to-one and one-to-many communications. It is clear to see that an encrypted one-to-one Telegram communication carries with it a reasonable expectation of being private. The complication comes from the one-to-many communication which has been historically popular with both ISIS[1016] and Neo-Nazis[1017] organising on the platform. Thus, this private Telegram channel is likely the one which the SIAs would find most necessary to their stated aims of protecting against threats to national security. The Court has stated that a person's reasonable expectations of privacy may be a significant – although not necessarily a conclusive – factor in whether there has been a violation of Article 8(1).[1018] The more important issue for the Court is whether and how the applicant's information was processed. Private life considerations may arise once any systemic or permanent record comes into existence, even if the methods used to gather said record are not intrusive or covert.[1019] In the context of bulk acquisition this data is used to create aggregated datasets which can be retained so long as they are necessary to a number of aims. This systemic record thus creates private life considerations from largely publicly available data. The public nature of an individual's data on Facebook and WhatsApp does not discount the creation of an interference with their Article 8 rights, and the creation of an identifying profile through the aggregation of their data compounds this interference.

10.3.5 The Double-Lock: A Flawed Safeguard

While the double-lock warrant authorisation system has been touted as an example for other bulk surveillance legislation, it contains a number of flaws to address. One issue with the double-lock system is the lack of *inter partes* argument, JCs will not hear representations by those adversely affected by the authorisation of the warrant.[1020] The absence of an adversarial challenge, or even a Special Advocate, means that the JC in question will have to both identify the arguments that might be advanced by those affected and then pass judgment on those arguments. Given this adversarial deficit, there is a danger that the JC will miss something which may have been put forward by the proposed subject of the warrant, or even by a Special Advocate for the proposed subject. It seems logical to assume that in the absence of an opposing voice, the question of what to consider when deciding the warrant will be influenced by the executive. The ECtHR noted in the first chamber judgment of *Centrum fur*

[1016] Nico Prucha, 'IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram' (2016) 10 Perspectives on Terrorism 48
[1017] https://www.bellingcat.com/news/2020/03/18/revealed-the-ukrainian-man-who-runs-a-neo-nazi-terrorist-telegram-channel/.
[1018] *P.G & J.H v UK* (2008) 46 EHRR para 57.
[1019] *P.G & J.H v UK* (2008) 46 EHRR para 60.
[1020] See chapter 4 on Judicial Authorisation.

Rattvisa that the presence of a privacy protection representative in the Swedish system of warrant authorisation, the Foreign Intelligence Court, compensated for the lack of transparency in the authorisation process.[1021] This representative cannot appeal against a decision made by the Foreign Intelligence Court or report any perceived irregularities to supervisory bodies, meaning that this compensation was limited in the Court's view. The representative is either a present or former permanent judge or attorney, has access to all case documents and may make statements. While they represent the interests of the general public rather than the subject of the warrant, the use of a representative like this would alleviate, in part, the lack of *inter partes* argument in the double-lock system. While this is a possible reform for the double-lock system it would not make the double-lock system entirely ECHR compatible as compatibility will still depend on the factual matrix of the specific case.

The second flaw with the double-lock is executive influence and the appearance of bias within the IPC. Key to the successful operation of the double-lock is the JC applying the correct amount of deference to the decisions of the executive. As discussed in chapter 7 this deference is contextual, adapting to the specific facts of the warrant. The danger of the JCs taking a more deferential approach to the authorisation of warrants is that it risks reducing the double-lock process to merely providing a thin veneer of legality to executive action. When the Secretary of State appeals the decision of a JC, the IPC concluded that the JC had not used the appropriate level of deference when reviewing the Secretary of State's decision. The IPC then took a more deferential approach to the warrant and approved it. In effect the Secretary of State has a second attempt on the basis that they did not receive their desired outcome. In this instance it resulted in a direct increase in deference from the IPC to the Secretary of State, but in other instances it may cause a JC to defer more to the Secretary of State on certain questions as they are liable to appeal if the JC takes too strict a view on one of the provisions of the warrant, or the decision process the secretary took in approving it.

This ability to appeal was compounded by the fact that the appointment and reappointment of the IPC is Prime Ministerial. Although this power is subject to the joint recommendations of the Lord Chief Justice of England and Wales, and their counterparts in the rest of the UK, the power to appoint remains in the hands of the executive.[1022] While it is unlikely due to the judicial character of the appointees that the IPC or a JC will be actively aligning their interests with the executive's it does present the appearance of bias.[1023]

[1021] Centrum paras 137- 138.
[1022] Joint Committee on Draft Investigatory Powers Bill paras 584 – 588.
[1023] *R v Bow Street Metropolitan Stipendiary Magistrate, ex parte Pinochet Ugarte (No. 2)* [2000] 1 AC 119, House of Lords para 132.

If the purpose of the JCs is to provide effective judicial oversight over the actions of the executive operating under the IPA, then it is unclear what justification there is for the power of appointment to remain in the hands of the executive. Following on from this point, there is the question of the conditions of the JC's re-appointment. Their re-appointment is subject to the joint recommendations outlined above. They are subject to three-year renewable terms which are simultaneously precarious and potentially indefinite. This produces a double incentive for the JC to act in accordance with the executive's wishes as there is the potential for indefinite employment should they please the executive. At the same time there is the possibility of being let go at the end of the three-year term.

Independent ex ante authorisation is an important safeguard in the ECtHR's view. In the GC judgment of *Big Brother Watch* the Court found that the major shortcoming under RIPA was the lack of ex ante independent authorisation which the Court described as "one of the fundamental safeguards".[1024] Under RIPA the Secretary of State alone authorised warrants, under the IPA this has been replaced with the so-called double-lock system. While this is certainly an improvement on RIPA it is not clear whether the double-lock will be sufficiently independent of the executive to meet this requirement. In their assessment of the RIPA system the Court noted that each application from the SIAs to the Secretary of State was subject to review by the agency making it prior to submission. While this additional scrutiny was viewed as valuable: "it remained the case that at the relevant time bulk interception conducted under the section 8(4) regime was authorised by the Secretary of State and not by a body independent of the executive".[1025] Considering the proximity of the JCs to the executive, and the influence the Secretary of State has over the institution, it is unclear whether the so called double-lock will always be sufficiently independent of the executive. The design of the system means that in certain circumstances it will not meet the requisite standards of independence.

Finally, there is the issue that the IPC also conducts the annual reporting of the authorisation and use of bulk powers. This highlights the problem with having a single person being responsible for both the authorisation of warrants and the annual reporting of their use. To date the reporting by the IPC has been forthcoming with details on errors, both minor and serious, on the part of SIAs utilising these warrants. However, it is within the power of the IPC to cover up their own errors through altering the reporting. The dual roles of overseeing the approval of warrants and the reviewing of the use of said warrants creates (at least the appearance of) a conflict of interest. This points to a need to separate these functions of the

[1024] BBW GC para 377.
[1025] Ibid.

IPC into two entities or at least two parts of the same organisation. One solution to this would be to separate the Investigatory Powers Commissioner from the other JCs. Under the Act the Commissioner is a JC in addition to their other roles.

10.3.6 Institutional Reform in the IPT

Chapter 8 highlighted a number of issues with the IPT. The first issue highlighted is that the Tribunal appears to be a remedy with an exceedingly low success rate for applicants. The Tribunal's response to this would rely first on their use of assumed facts in an open session to mitigate this lack of clarity in the closed session. Second, they would likely take the position that as it is free to apply to the IPT, individuals without real cause to believe they are subject to surveillance can bring claims to it. These contribute to the large proportion of 'frivolous and vexatious' rulings.

This low success rate likely stems from two sources. First, the reliance on the 'no determination' outcome. This outcome has a dual meaning which would likely cover the majority of complaints to the IPT: either no surveillance took place or legal surveillance took place and to reveal it would jeopardise national security or the continued operation of a SIA. The distance between these two meanings is broad enough that it is near impossible for applicants to know the truth of whether they have been subjected to the use of investigatory powers under the Act. The counterargument to this is that the IPT would hold that given the legitimate national security interests it was necessary to protect the operation of the SIAs and not notify applicant's if revealing their subjection to investigatory powers would be detrimental to national security. Nonetheless there is a distinct lack of procedural justice provided by the IPT to its applicants which could be remedied through the use of special advocates acting on behalf of the claimants in the closed session. In this way, the claimant would have a greater belief that they were given a fair opportunity to plead their case, even without seeing the actual evidence held on them.

The second issue with the IPT is the large amount of influence the Secretary of State holds over the IPT. While the rules of the Tribunal are set out in the Investigatory Powers Tribunal Rules 2018, RIPA itself states that the IPT shall, subject to rules made by the Secretary of State under section 69(1), determine its own procedure in respect of complaints. This is understood as meaning that the IPT can issue its own rules but also that it may alter them depending on the circumstances.[1026] This is most easily explained as being a form of discretion conferred on the Secretary of State by RIPA.[1027] The rule-making power of the

[1026] Alisdair Gillespie and Siobhan Weare, *The English Legal System* (7th edn. OUP 2019).
[1027] In the Matter of Applications Nos IPT/01/62 and IPT /01/77 (2003) Para 36.

Secretary of State is a wide one, as they may make rules regulating the exercise by the Tribunal of the jurisdiction conferred on them by section 65 RIPA. Although particular types of provision potentially covered by the exercise of power to make rules are set out, the particular topics singled out for special mention are "without prejudice to the generality" of the discretion of the Secretary of State.[1028] The use of this discretion by the Home Secretary took the form of the original, and updated, IPT Rules which place a number of duties on the Tribunal including a general duty to restrict disclosure of information.[1029] If the IPT is to constitute an effective check on the executive in the use of investigatory powers, this discretion should either be removed or sufficiently narrowed through the use of a further update to the IPT rules.

Finally, the third issue is the inability for the IPT to place a binding obligation on the executive. In order to be effective "a remedy must be capable of remedying directly the impugned state of affairs and must offer reasonable prospects of success."[1030] In *Kennedy* the Court had found that the IPT could consider complaints about the general compliance of the surveillance regime with the Convention and could make a finding of incompatibility if necessary. However, such a finding of incompatibility did not give rise to a binding obligation on the Government to remedy said incompatibility to benefit the applicant.[1031] In the first chamber judgment of *Big Brother Watch* the Court reversed this *Kennedy* ruling, holding that the practice of the Government giving effect to the IPT's finding on the incompatibility of domestic law with the Convention was sufficiently certain for it to be considered an effective remedy.[1032] The Court added that the IPT's effectiveness was bolstered by its ability to reference a case, as a matter of EU law, to the CJEU, which could then impose a binding obligation on the UK Government.[1033] This ruling was not challenged, and therefore not considered, in the Grand Chamber proceedings because the circumstances arose when appeal to the CJEU was available.[1034] This absence of the CJEU post-Brexit presents an issue for the IPT. Without this external source of binding obligations on the executive, the ability for the IPT to act as an effective domestic remedy remains within the discretion of the executive. While the Government thus far has chosen to treat the decisions of the IPT as though they were binding, they could choose not to if it became more politically expedient to do so. As part of the proposed update to the IPT rules, the IPT should be given the ability to place a

[1028] RIPA 2000 s 69(2).
[1029] IPT Rules, r 6.
[1030] *Kennedy v. UK* (2011) 52 EHRR 4 para 109.
[1031] Ibid.
[1032] Big Brother Watch paras 255 – 257.
[1033] Ibid para 263.
[1034] Big Brother Watch (GC) para 271.

binding obligation on the actions of the Home Secretary in regards to the use of investigatory powers.

10.7 Future Research and Limitations

This thesis has found that the safeguards present in the IPA are likely to meet both the standards of the ECtHR and the CJEU, while simultaneously showing that these safeguards do not adequately protect against the multivariate harms caused by the use of bulk powers. As a result, the approaches of the ECtHR, CJEU and IPA all fail to adequately reflect the differences between these powers. This points to a broader question of whether it is possible for such wide surveillance powers to be compatible with the general principles underlying these sources of human rights law.

This thesis is limited to the cases which have occurred up until 2023. However, this is a field of law which is likely to change as more challenges appear before the national and supranational courts. For example, as of the writing of this thesis the there is an ongoing challenge to the compatibility of the IPA with ECHR and CFR by the privacy NGO Liberty. As of August 2023, this challenge was decided in the Court of Appeal. A future analysis of this challenge is essential to the findings of this thesis as it concerns the compatibility of the UK bulk powers regime with both the ECHR and retained EU law.

As chapter 4 has shown, each bulk surveillance power is qualitatively different from the other in terms of the level of intrusion to a given individual, the way that data is collected and the ability to aggregate said retained data. Future work should focus on how to design safeguards which reflect these differences. While it is difficult to say whether these theoretical safeguards could limit the use of these powers sufficiently so as to be compatible with general principles of human rights or to significantly reduce the harms of the existence and use of these powers, more work on identifying the specific harms of these powers and how to protect against them will have an impact on the average level of protection provided to a given individual against them. Chapter 4 did not go into detail as to the specific harms of bulk acquisition, bulk equipment interference and bulk personal datasets in the same level of detailed analysis as the bulk interception analysis provided in chapter 3. Future work should tease out the specific harms of these powers in order to properly safeguard against their harms.

Given the imperceptibility of the double-lock process to outside observers it is difficult for this thesis to give a clear answer on how well this key safeguard is functioning. Future research could answer this question through the use of more hands-on qualitative methods such as ethnography and interviewing judicial commissioners. This would require adequate

security clearance and would likely be limited in scope however it would be invaluable to the public understanding of this safeguard which carries a large amount of weight for the safeguarding of the Investigatory Powers Act 2016. Similarly, another limitation of this thesis is that the impact of other oversight mechanisms provided by the IPC such as auditing and reporting are difficult to assess from an outside perspective. The use of such methods in a future project would help to alleviate this limitation. While the procedural justice analysis of the IPT provided in chapter 8 shows how an applicant is likely to feel a lack of both substantive and procedural justice when they apply to the IPT as their sole domestic remedy, it was limited by its inability to interview or survey those who apply to the IPT. Some form of quantitative survey or qualitative interviewing of IPT applicants would go far to prove the distinct lack of procedural justice provided by the IPT.

10.8 Conclusion

This thesis set out to answer two questions: whether the bulk surveillance powers contained within the Investigatory Powers Act 2016 are compatible with European human rights law, and whether the protection provided by human rights law is capable of protecting against the harms of bulk surveillance powers. In chapters 3 and 4 this thesis showed how the harms caused by the existence and operation of these bulk powers causes a variety of individual and societal harms. These chapters showed the breadth and depth of scope of these powers and how each is qualitatively different in terms of impact and reach. In chapters 6 and 7 a systematic analysis of both the ECtHR and CJEU's caselaw on this subject showed that both sources of European human rights law allow for the use of these powers provided they meet a set of minimum requirements against abuse. These parallel sets of minimum requirements are similar in effect to each other. Chapters 8 and 9 showed that the interlocking suite of safeguards present in the IPA is both deeply flawed, unable to protect against the harms of bulk surveillance, and yet are likely to meet the requirements set by the ECtHR and CJEU. This points to a larger issue wherein European human rights law is unable to protect against the harms of bulk surveillance while simultaneously sanctioning its use as necessary.

Cases

A v Secretary of State for the Home Department [2005] 2 AC 68

A v Secretary of State for the Home Department [2004] UKHL 56

A v Secretary of State for the Home Department [2004] QB 335

AB v Hampshire Constabulary [2019] UKIPTrib 17_191-C

Akdiver v Turkey (1997) 23 EHRR 143

Al Jedda v Secretary of State for the Home Department, SIAC judgment of April 7, 2009

Al-Rawi v Security Service [2011] UKSC 34

B v France (1993) 16 EHRR 1

Bank Mellat v HM Treasury (No2) [2014] AC 700

Banković and Others v. Belgium (2007) 44 EHRR SE5

Barbulescu v Romania App no 61496/08 (ECtHR 5 September 2017)

Belgian Linguistics Case (No 2) (1968) 1 EHRR 252

Belhadj v Security Service [2015] UKIPTrib 13_132-H

Big Brother Watch and Others v. The United Kingdom App nos 58170/13, 62322/14 and 24960/15, (ECHR, 13 September 2018)

Big Brother Watch v United Kingdom (GC) App nos 58170/13, 62322/14, 24960/15 (ECtHR 25 May 2021)

Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi v Ireland (2006) 42 EHRR 1

Botta v Italy (1998) 26 EHRR 241

Boultif v Switzerland 2001-IX; 33 EHRR 1179

Buckley v United Kingdom (1997) EHRR 101

Buglov v. Ukraine App no 28825/02 (ECtHR 10 July 2014)

C.R. v UK (1995) Series A no 335-C

Campbell v. the United Kingdom (1992) 15 EHRR 137

Catt v UK (2019) 69 EHRR 7

Centrum för Rättvisa v Sweden (2018) 68 EHRR 2

Centrum för Rättvisa v Sweden (GC) App no 35252/08 (ECtHR 25 May 2021)

CF v Security Service [2013] EWHC 3402 (QB)

Chahal v UK 23 EHRR 413

Chatwani v National Crime Agency [2015] UKIPTrib 15_84_88-CH [2015] UKIPTrib 15_84_88-CH

Chief Constable of Midlands Police, ex parte Wiley [1995] 1 AC 274

Christine Goodwin v the United Kingdom (28957/95) (Unreported, July 11, 2002) (ECHR)

Ciubotaru v. Moldava, App No 27138/04 (ECtHR 27 April 2010)

Copland v United Kingdom App no 62617/00 (ECtHR 3 April 2007)

Cotlet v Romania (38565/97) (Unreported, June 3, 2003) ((ECHR))
Council of Civil Service Unions and Others v Minister for the Civil Service [1985] AC 274
Davies v British Transport Police [2018] UKIPTrib IPT_17_93-H
Davis [1993] 1 WLR 613
De Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing [1999] 1 AC 69
Delcourt v Belgium (1979-80) 1 EHRR 355
Dias and Matthews v Cleveland Police [2017] UKIPTrib 15_586-CH
Digital Rights Ireland Ltd v Minister for Communications [2015] Q.B. 127
Dimes v. Proprietors of Grand Junction Canal (1852) 3 HL Cas 759
Doerga v. the Netherlands (2005) 41 EHRR 4
Dudgeon v The United Kingdom App no 7525/76 (ECtHR 22 October 1981)
Dunn v Durham County Council [2013] 1 WLR 2305
Edwards and Lewis v. UK (2005) 40 EHRR 24
Edwards v United Kingdom (1992) 15 EHRR 417
Esbester v United Kingdom (1994) 18 EHRR CD72
Fernandez Martinez v Spain [GC] (2015) 60 EHRR 3
Gaskin v. the United Kingdom 7 July 1989, Series A no 160
Golder v United Kingdom (1979-80) 1 EHRR 524
H [2004] 2 AC 134
Halford v. the United Kingdom 25 June 1997, Reports of Judgments and Decisions 1997-III
Handyside v UK (1979-80) 1 EHRR 737
Hatton v UK, (2003) 37 EHRR 611
Human Rights Watch [2016] UKIPTrib 15_165-CH
Huvig v. France (1990) 12 EHRR 528
In the Matter of Applications Nos IPT/01/62 and IPT/01/77 (2003)
Incal v Turkey (2000) 29 EHRR 449
James v UK (1986) 8 EHRR 123
Joined Cases C-203/15 and C-698/15 Tele2 Sverige [2017] Q.B. 771
Kay v Lambeth London Borough Council [2006] 2 AC 465
K and T v Finland [GC] 2001-VII; 36 EHRR 255
Kennedy v Information Commissioner (2014) 2 WLR 808
Kennedy v United Kingdom (2011) 52 EHRR 4
Klass and Others v. Germany (1979-80) 2 EHRR 214
Klaus Müller v. Germany App no 24173/18 (ECHR 19 November 2020)
Kruslin v France 12 EHRR 547

La Quadrature du Net v Premier Ministre (C-511/18) [2021] 1 W.L.R. 4457
Le Compte, van Leuven and de Meyere v Belgium (1982) 4 EHRR 1
Leander v Sweden (1987) 9 EHRR 433
Lebois v. Bulgaria no 67482/14 (ECHR 19 October 2017)
Liberty [2014] UKIPTrib 13_77-H
Liberty v Secretary of State [2020] 1 WLR 243
Liberty v United Kingdom (2009) 48 EHRR 1
Makanjuola v Commissioner of Police of the Metropolis [1992] 3 AII ER 617
Malone v United Kingdom (1985) 7 EHRR 14
Marckx v Belgium A 31 (1979); (1979–80) 2 EHRR 305
Martinie v France App no 58675/00 (Grand Chamber, 12 April 2006)
Michaud v. France App no 12323/11 (ECtHR 6 December 2012)
Mikulic v Croatia (2002) 2 WLUK 216
Ministerio dell'Economica e delle Finanze v Paint Graphos Sarl (C-78-80/08) [2011] ECR I-7611
MM v United Kingdom App no 24029/07 (ECtHR 13 November 2012)
Modinos v Cyprus App no 15070/89 (ECtHR 22 April 1993)
Mustafa Sezgin Tanrukulu v. Turkey App no 27473/06 (ECtHR 18 July 2017)
National and Local Government Officers' Association (1992) 5 Admin LR 785
National Council for Civil Liberties (Liberty), R (On the Application Of) v Secretary of State for the Home Department & Anor (2022) EWHC 1630 (Admin)
News Group [2015] UKIPTrib 14_176-H
Niemietz v Germany App no 13710/88 (ECtHR 16 December 1992)
Norris v Ireland App no 10581/83 (ECtHR 26 October 1988)
Nuri Kurt v Turkey (2007) 44 EHHR 36
Ocalan v Turkey [GC] (2005) 41 EHRR 45
Odievre v France (2004) 38 EHRR 43
Olsson v Sweden (1989) 11 EHRR 259
Osborn v. The Parole Board [2013] UKSC 61
P.G & J.H v UK (2008) 46 EHRR para 57
Paton and others v Poole Borough Council [2010] (IPT/09/01 02 03 04 and 05)
Paton and others v Poole Borough Council [2010] (IPT/09/01 02 03 04 and 05)
Peck v UK (2003) 36 EHRR 41
Pham v Secretary of State for the Home Department [2015] 1 WLR 1591
Pham v Secretary of State for the Home Department [2015] UKSC 19
Piechowicz v. Poland App no 20071/07 (ECtHR 17 April 2012)

Pierre Herbecq and the Association Ligue des droits de l'Homme v Belgium App no 32200/96 and 32201/96 (ECtHR 14 January 1998)

Piersack v Belgium (1983) 5 EHRR 169

Police Scotland [2016] UKIPTrib15_602-CH

Privacy International & Greennet [2016] UKIPTrib 14_85-CH

Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ [2016] UKIPTrib 14_85-CH,

Proceedings brought by Ministero Fiscal [2019] 1 W.L.R.

R (Ali Zaki Mousa) No.2 [2013] EWHC 1412 (Admin)

R (Ali Zaki Mousa) No.2 [2013] HRLR 13

R (Baiai and another) v Secretary of State for the Home Department (Nos 1 and 2) [2008] QB 143

R (Daly) v Secretary of State for the Home Department [2001] 2 AC 532

R (Daly) v Secretary of State for the Home Department [2001] 2 AC 532

R (Lord Carlile of Berriew QC) v Secretary of State for the Home Department [2014] UKSC 60

R (Nicklinson) v Ministry of Justice [2014] UKSC 38

R (Nicklinson) v Ministry of Justice [2015] AC 657

R (on the application of Gillan) v Commissioner of Police for the Metropolis [2006] UKHL 12

R (on the application of Lord Carlile of Berriew QC and others) v Secretary of State for the Home Department [2014] UKSC 60

R (Razgar) v Secretary of State for the Home Department [2004] 2 AC 368

R v Bow Street Metropolitan Stipendiary Magistrate, ex parte Pinochet Ugarte (No. 2) [2000] 1 AC 119, House of Lords

R (Liberty) v Secretary of State [2022] 1 W.L.R. 4929

R v Ministry of Defence, ex p Smith [1996] QB 517

R v Secretary of State for the Home Department, ex p Brind [1991] 1 AC 696

R v Secretary of State for the Home Department, Ex p Leech [1994] QB 198

R. (Corner House Research and Another) v Director of the Serious Fraud Office [2008] UKHL 60

R. (on the application of Secretary of State for the Home Department) v Bullivant [2008] EWHC 337 (Admin)

R (Open Rights Group Ltd) v Secretary of State for the Home Department [2022] QB 166

R. v Secretary of State for the Home Department Ex p Fire Brigades Union [1995] 2 AC 513

R. v. Inland Revenue Commissioners, ex p. National Federation of Self-employed and Small Businesses Ltd [1982] AC 617
Re MB [2006] EWHC 1000 (Admin)
Rees v. The United Kingdom (1987) 9 EHRR 56
Roche v. the United Kingdom [GC] App no 32555/96, ECHR 2005-X
Rotaru v Romania App no 28341/95 (ECtHR 4 May 2000)
S and Marper v United Kingdom (2008) 48 EHRR 1169
Salontaji-Drobnjak v. Serbia App No 36500/05 (ECtHR 13 October 2009)
Schonenberger and Durmaz v. Switzerland (1989) 11 EHRR 202
Science Research Council v Nassé [1979] QB 144
Secretary of State for Education and Science v Tameside Metropolitan Borough Council [1977] AC 1014
Secretary of State for the Home Department (Appellant) v. JJ and others (FC) (Respondents) [2007] UKHL 45
Secretary of State for the Home Department v AF and others [2009] UKHL 28
Secretary of State for the Home Department v GG [2009] EWHC 142 (Admin)
Secretary of State for the Home Department v Lord Alton of Liverpool [2008] EWCA Civ 443
Secretary of State for the Home Department v Lord Alton of Liverpool [2008] 1 WLR 2341
Secretary of State for the Home Department v MB [2006] EWCA Civ 1140
Secretary of State for the Home Department v Rehman [2001] UKHL 47
Secretary of State for the Home Department v Rehman [2003] 1 AC 153
Segerstedt-Wiberg v Sweden (2007) 44 EHRR 2
Sejdovic v Italy (2004) 42 EHRR 360
Sekanina v. Austria 25 August 1993, § 25, Series A no 266-A
Shtukaturov v. Russia App no 44009/05 (ECHR 27 March 2008) App no 44009/05 (ECHR 27 March 2008)
Silver and Others v United Kingdom (1981) 3 EHRR 475
Silver and Others v. the United Kingdom 25 March 1983, Series A no 61
Sisojeva v Latvia (2007) 45 EHRR 33
Slivenko v Latvia (2004) 39 EHRR 24
Smith and Grady v UK (1999) 29 EHRR 493
Soering v UK (1989) 11 EHRR 439
Sporrong and Lonnroth v. Sweden (1983) 5 EHRR 35
Sunday Times v United Kingdom (1979-80) 2 EHRR 245
Szabó and Vissy v Hungary (2016) 63 EHRR 3
Szuluk v. United Kingdom App no 36936/05 (ECtHR 2 June 2009)

Taskin v. Turkey (2006) 42 EHRR 50

Turek v. Slovakia, App No 57986/00 (ECtHR 14 February 2006)

Tysiac v Poland App No 5410/03 (ECtHR 20 March 2007)

Vaughan v South Oxfordshire District Council [2012] IPT/12/28/C

Vincent C Frank-Steiner v the Secret Intelligence Service [2008] (IPT/06/81)

Vogt v Germany (1996) 21 EHRR 205

Von Hannover v Germany [GC] (2012) 55 EHRR 15

Weber and Saravia v Germany (2008) 46 EHRR SE5

X and Y v. The Netherlands App no 8978/90 (ECtHR 26 March 1985)

Z v. Finland 25 February 1997, Reports of Judgments and Decisions 1997-I

Zaiet v Romania (2016) 62 EHRR 9

Zakharov v Russia (2015) 63 EHRR 17

Legislation and Codes of Practice

EU General Data Protection Regulation

Human Rights Act 1998

Investigatory Powers Tribunal Rules 2000

Regulation of Investigatory Powers Act 2000

Home Office, *Bulk Acquisition of Communications Data Code of Practice*, 2018)

Home Office, *Equipment Interference Code of Practice* 2018)

Home Office, *Intelligence services' retention and use of bulk personal datasets* (2018)

Home Office, *Interception of Communications Code of Practice* (2018)

European Union, Consolidated version of the Treaty on the Functioning of the European Union, 26 October 2012, OJ L. 326/47-326/390; 26.10.2012

Bibliography

Journal Articles

Abbasli E, 'The Protection of the Freedom of Expression in Europe: Analysis of Article 10 of the ECHR.' (2015) 2 Baku St UL 18

Allan TRS, 'Human Rights and Judicial Review: A Critique of "Due Deference"' (2006) 65 Cambridge Law Review 671

Arnull, A 'Owning up to Fallibility: Precedent and the Court of Justice' (1993) 30 CMLRev 247.

Aston, V., 'State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protester perspectives' (2017) 8 European Journal of Law and Technology 1.
Ann Bartow, ‘A feeling of unease about privacy law.’ (2006) 154 U. PA. L. Rev. 477
Bernal, P., 'Data gathering, surveillance and human rights: recasting the debate' (2016) 1 Journal of Cyber Policy 243.
Bondy V and Sunkin M, 'Accessing Judicial Review' (2008) 4 Public Law 674
Boon A and Nash S, 'Special Advocacy: Political Expediency and Legal Roles in Modern Judicial Systems’ (2006) 9 Legal Ethics 101
Boukalas C, 'Overcoming liberal democracy:“Threat governmentality” and the empowerment of intelligence in the UK investigatory powers Act' (2020) 82 Studies in Law, politics, and society 1
Brems E and Lavrysen L, 'Procedural justice in human rights adjudication: The European Court of Human Rights.' (2013) 35 Human Rights Quarterly 176
Buchi,M., Festic, N., and Latzer, M 'The chilling effects of digital dataveillance: a theoretical model and an empirical research agenda' (2022) 9 Big Data & Society 1.
Buono, I and Taylor, A "Mass surveillance in the CJEU: forging a European consensus." *The Cambridge Law Journal* 76, no. 2 (2017): 250-253.
Bygrave LA, 'Data protection pursuant to the right to privacy in human rights treaties' (2008) 6 International Journal of Law and Information Technology 247
Cayford M and Pieters W, 'The effectiveness of surveillance technology: What intelligence officials are saying ' (2018) 34 The Information Society 88
Cayford M, Pieters W and Hijzen C, 'Plots, murders, and money: oversight bodies evaluating the effectiveness of surveillance technology' (2018) 33 Intelligence and national security 999
Chamberlain M, ‘Special Advocates and procedural fairness in closed proceedings’ (2009) 28 Civil Justice Quarterly 314
Connelly AM, 'Problems of interpretation of Article 8 of the European Convention on Human Rights.' (1986) 35 International & Comparative Law Quarterly 567
Cornford T and Sunkin M, ' ‘The Bowman Report, Access and the Recent Reforms of the Judicial Review Procedure’ (2001) 11 Public Law
Davies G, 'Shining a light on policing of the dark web: an analysis of UK investigatory powers' (2020) 84 The Journal of Criminal Law 407
De Hert P and Malgieri G, '"Article 8 ECHR Compliant and Foreseeable Surveillance: The ECTHR's Expanded Legality Requirement Copied by the CJEU. A Discussion of European Surveillance Case Law.' (2020) 6 ECLAN Volume, Forthcoming, Brussels Privacy Hub Working Paper

Edwards L and Urquhart L, 'Privacy in public spaces: what expectations of privacy do we have in social media intelligence?' (2016) 3 International Journal of Law and Information Technology

Edwards RA, '"Judicial Deference under the Human Rights Act.' (2002) 65 The Modern Law Review

Elliot M, 'Proportionality and Deference: The Importance of a Structured Approach' (2013) University of Cambridge Faculty of Law Research Paper No. 32/2013, Available at SSRN: https://ssrn.com/abstract=2326987 or http://dx.doi.org/10.2139/ssrn.2326987

Ferguson G and Wadham J, 'Privacy and surveillance: a review of the Regulation of the Investigatory Powers Act 2000.' (2003) European Human Rights Law Review 101

Flinders M and Kelso A, ''Mind the Gap: Political Analysis, Public Expectations, and the Parliamentary Decline Thesis'' (2011) 13 British Journal of Politics and International Relations 249

Foster S, ''Stop me if you've heard this one before: judicial deference in free speech and security cases'' (2015) 20 Cov L J 58

Galetta A and De Hert P, 'Complementing the surveillance law principles of the ECtHR with its environmental law principles: An integrated technology approach to a human rights framework for surveillance' (2014) 10 Utrecht Law Review 55

Gerards J, '"How to improve the necessity test of the European Court of Human Rights."' (2013) 11 International journal of constitutional law 466

Goodman T, 'The Investigatory Powers Act 2016: A Victory for Democracy and the Rule of Law' (2018) 5 Bristol Law Review 2

Granger MP and Irion K, 'The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39 European Law Review 834

Hooper H, 'The future is foreign country' (2015) 74 CLJ 23

Hughes K, 'Mass surveillance and the European Court of Human Rights' (2018) 6 EHRLR 589

Jackson J, 'The role of special advocates: Advocacy, due process and the adversarial tradition.' (2016) 20 The International Journal of Evidence and Proof 343

Kavanagh A, 'CASES: Special Advocates, Control Orders and the Right to a Fair Trial.' (2010) 73 The Modern Law Review 836

Kavanagh A, "Constitutionalism, Counterterrorism, and the Courts: Changes in the British Constitutional Landscape' (2011) 9 International Journal of Constitutional Law 172.

Kavanagh A, ''Judicial Restraint in the Pursuit of Justice'' (2010) 60 University of Toronto Law Journal 23

King J, '‘The Justiciability of Resource Allocation’ (2007) 70 Mod. L. Rev. 198
Macdonald S, '‘The role of the courts in imposing terrorism prevention and investigation measures: normative duality and legal realism’ (2015) 9 Criminal Law and Philosophy 265
McHarg A, 'Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights' (1999) 62 Modern Law Review 671
Macnish, K. 'Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World' (2018) 35 Journal of Applied Philosophy 2.
Moore M, '"RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework"' (2014) 85 The Political Quarterly 125
Mowbray A, 'The Creativity of the European Court of Human Rights' (2005) 1 Human Rights Law Review 57
Murphy CC, '"Counter-terrorism and the culture of legality: the case of special advocates."' (2013) 24 King's Law Journal 19
Murphy MH, 'A Shift in the Approach of the European Court of Human Rights in Surveillance Cases: A Rejuvenation of Necessity?' (2014) 5 EHRLR 515
Murphy MH, 'Algorithmic surveillance: the collection conundrum' (2017) 31 International Review of Law, Computers & Technology
Murray D and Fussey P, 'Bulk surveillance in the digital age: Rethinking the human rights law approach to bulk monitoring of communications data' (2019) 52 Israel Law Review 31
Murray H, 'Judicial Review after the Human Rights Act' (1999) 2 QMWLJ 14
Palmisano M, 'The surveillance cold war: Recent decisions of the european court of human rights and their application to mass surveillance in the united states and Russia' (2017) 20 Gonzaga Journal of International Law 75
Pannick D, 'Principles of Interpretation of Convention Rights under the Human Rights Act and the Discretionary Area of Judgment' (1998) 98 Public Law 545
Penney, J. 'Chilling Effects: Online Surveillance and Wikipedia Use' (2017) 31 Berkeley Technology Law Journal 118
Prucha N, 'IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram' (2016) 10 Perspectives on Terrorism 48
Richards, N. 'The Dangers of Surveillance' (2012) 126 Harv L Rev 1934.
Richards, N. 'Intellectual Privacy' (2008) 87 Tex L Rev 387
Rosen J, 'The Right to be forgotten' (2011) 64 Stan L Rev Online 88
Schafer B, 'Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill' (2016) 40 Datenschutz und Datensicherheit-DuD 592

Scaramuzza T, 'Judicial deference versus effective control: the English courts and the protection of human rights in the context of terrorism' (2006) 11 Coventry Law Journal 2
Schauer, F. 'Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect"' (1978) 58 BU L REV 685.
Scott PF, 'Hybrid institutions in the national security constitution: the case of the Commissioners.' 39 Legal Studies 432
Scott PF, 'Ouster clauses and national security: judicial review of the investigatory powers tribunal' (2017) 17 Public Law 355
Siatitsa, I., 'Freedom of assembly under attack: General and indiscriminate surveillance and interference and internet communications' (2020) 102 International Review of the Red Cross 181.
Daniel Solove, 'A Taxonomy of Privacy' (2006) 154 U. PENN. L. REV 477
Daniel Solove 'Why privacy matters even if you have nothing to hide.' (2011) Chronicle of Higher Education 15
Stevens, A., Fussey, P., and Saki, O. "I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe' (2023) 10 Big Data & Society 1.
Stoycheff, E, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) 93 Journalism and Mass Communication Quarterly 296.
Stoycheff, E. 'Cookies and content moderation: affective chilling effects of internet surveillance and censorship ' (2023) 20 Journal of Information Technology & Politics 113.
Thompson N and others, 'Cultural factors and the role of privacy concerns in acceptance of government surveillance.' (2020) 71 Journal of the Association for Information Science and Technology 1129
Tomkins A, 'Justice and Security in the United Kingdom' (2014) 47 Israel Law Review 305
Tomkins A, 'National Security and the role of the court: a changed landscape?' (2010) 126 LQR 543
Torkjazi M, Rejaie R and Willinger W, 'Hot today, gone tomorrow: on the migration of MySpace users.' (2009) Proceedings of the 2nd ACM workshop on Online social networks
Tyler RT, 'Procedural Justice, Legitimacy, and the Effective Rule of Law.' (2003) 30 Crime and Justice 284
Van der Velden L, 'Leaky apps and data shots: Technologies of leakage and insertion in NSA-surveillance' (2015) 13 Surveillance & Society 182
Vogiatzoglou P, ''Centrum for Rattvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy'' (2018) 4 Eur Data Prot L Rev 563

Ullrich, P., and Wollinger, GR. 'A surveillance studies perspective on protest policing: the case of video surveillance of demonstrations in Germany' (2011) 3 Interface: a journal for and about social movements 12.
Waldron J, 'How Law Protects Dignity' (2012) 71 CLJ 200
Wicker, S and Ghosh, D. 'Reading in the Panopticon - Your Kindle May Be Spying on You, But You Cannot Be Sure' (2020) 63 Communications of the ACM 68.
Williams R, 'Structuring Substantive Review.' (2017) 1 Public Law 99
Wilson K, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto itself?' (2020) 23 Trinity CL Rev 129
Waranch RS, 'Digital Rights Ireland Deja Vu: Why the Bulk Acquisition Warrant Provisions of the Investigatory Powers Act 2016 Are Incompatible with the Charter of Fundamental Rights of the European Union' (2017) 50 George Washington International Law Review 209
Woods L, McNamara L and Townend J, '"Executive accountability and national security." ' 84 The Modern Law Review 553
Woolf L, "Current Challenges in Judging" (Fifth Worldwide Common Law Judiciary Conference, Sydney, 10 April 2003)
Young JM, 'Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation. ' (2004) 9 International Journal of Communications Law & Policy

Parliamentary Debates

HC Deb 15 November 2015, vol 601, cols 969-972
HC Deb 15 November 2015, vol 601, cols 972-974
HC Deb 6 June 2016, vol 611, col 1148.
HL Deb 7 September 2016, vol 774, col 1047.

Submitted Evidence

Amnesty International UK, – *supplementary written evidence (IPB0074)*
Anderson D, *Supplementary Written Evidence (IPB0152)*
Bar Council, *Bar Council – supplementary written evidence (IPB0134)*
Brown I, 'Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK ' https://ssrn.com/abstract=2336609
Hickman T, *Written Evidence (IPB0039)*
Justice, *Justice – written evidence (IPB0148)*
Justice, *Secret Evidence* (Justice 2009)
Bingham Centre for the Rule of Law, *Written Evidence (IPB0055)*

Amberhawk Training Limited, *Amberhawk Training Limited – written evidence (IPB0015)*
London Internet Exchange, *London Internet Exchange (LINX) – written evidence (IPB0097)*
Lord Williams of Mostyn, *HL Debs 5 June 1997, col. 736*
McEvedys Solicitors & Attorneys Ltd, *McEvedys Solicitors & Attorneys Ltd – written evidence (IPB0138)*
QC LCoBC, *Written Evidence (IPB00117)*
UN Special Rapporteurs, *UN Special Rapporteurs – written evidence (IPB0102)*
Telecom B, *BT – supplementary written evidence (IPB01151)*

Reports
Anderson D, *A Question of Trust - Report of the Investigatory Powers Review* (2015)
Anderson D, *Report of the Bulk Powers Review* (2016)
House of Commons Constitutional Affairs Committee *The Operation of the Special Immigration Appeals Commission* ((2004-05, HC 323-2), Ev 80,, (2004-05))
House of Commons Public Administration Select Committee, *Good Government* ((HC 97 2008–09))
Investigatory Powers Commissioner's Office, *Annual Report*, (2017)
Investigatory Powers Commissioner's Office, *IPCO Press release,18 October 2017* (2017)
Investigatory Powers Commissioner's Office, *Annual Report*, 2018)
Investigatory Powers Commissioner's Office, *IPCO Report 2018* 2018)
Investigatory Powers Commissioner's Office, *Annual Report of the Investigatory Powers Commissioner*, 2019)
Interception of Communications Commissioner's Office, *Interception of Communications Commissioner's Office—written evidence (IPB0101)*
Investigatory Powers Commissioner's Office, *Advisory Note*, (2017)
Investigatory Powers Commissioner's Office, *Annual Report*, (2017)
Investigatory Powers Tribunal, *Investigatory Powers Tribunal Report 2010*, 2010)
Joint Committee on the Draft Investigatory Powers Bill, *Draft Investigatory Powers Bill Report* (HL Paper 93 HC 651 2016)
National Security Agency, *Slide no. 3 of the NSA presentation: Working principle of Upstream and PRISM (FAA702 Operations. Two Types of Collection.)* (2013)
Privacy International, *When Local Authorities aren't your Friends*, (2020) https://privacyinternational.org/campaigns/when-local-authorities-arent-your-friends accessed 10/06/2022
Public Interest Monitor, *Report of the Public Interest Monitor, October 2006*, (2006)

Rainey B, Wicks E and Ovey C, *Jacobs, White and Ovey: The European Convention on Human Rights* (7th edn, Oxford University Press 2017)
UK Cabinet Office, *'The Justice and Security Green Paper'* ((London, 4 April 2012), 2012)
The Intelligence and Security Committee, *Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme* (2013)

Newspaper Articles

Ball J, Harding L and Garside J, 'BT and Vodafone among Telecoms Companies Passing Details to GCHQ' *The Guardian* (2013) (https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq)
Brandom R, 'FBI agents tracked Harvard bomb threats despite Tor' (*The Verge,* 2013) https://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor accessed 02/12/2021
Champion M, 'This is what it's like to be wrongly accused of being a paedophile because of a typo by police' *Buzzfeed News* (2017) (https://buzzfeed.com/matthewchampion/this-mans-life-was-destroyed-by-a-police-typo) accessed 02/12/2021
Colborne M, 'Revealed: The Ukrainian Man Who Runs A Neo-Nazi Terrorist Telegram Channel' *Bellingcat* (2020) https://www.bellingcat.com/news/2020/03/18/revealed-the-ukrainian-man-who-runs-a-neo-nazi-terrorist-telegram-channel/ accessed 07/06/2022
Gallagher R, 'Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities' *The Intercept* (2015) (https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/) accessed 02/12/2021
Gallagher R and Greenwald G, 'How the NSA plans to infest 'millions' of computers with malware' *The Intercept* (2014) (https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ accessed 02/12/2021
Greenwald G and MacAskill E, 'NSA Prism program taps in to user data of Apple, Google and others' *The Guardian* (2013) (https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data) accessed 02/12/2021
Intercept T, 'Pull Through Steering Group Minutes' *The Intercept* (2015) <https://theintercept.com/document/2015/09/25/pull-steering-group-minutes/> accessed 07/06/2022
MacAskill E and others, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian* (2013) (https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa accessed 02/12/2021

MacAskill E and others, 'How does GCHQ's internet surveillance work?' *The Guardian* (2013) (https://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work accessed 02/12/2021

Markoff J and Shane S, 'Documents Show Link Between AT&T and Agency in Eavesdropping Case' *The New York Times* (2006) (https://www.nytimes.com/2006/04/13/us/nationalspecial3/13nsa.html) accessed 07/06/2022

Martin AJ, 'Blighty's GCHQ stashes away 50+ billion records a day on people' *The Register* (2015) (https://www.theregister.co.uk/2015/09/25/trillions_in_surveillance_gchq/) accessed 07/06/2022

Sedley S, 'Judicial Politics' *London Review of Books* (2012) http://www.lrb.co.uk/v34/n04/stephen-sedley/judicial-politics accessed 07/06/2022

Spiegel Online, 'Inside TAO: Documents Reveal Top NSA Hacking Unit' *Spiegel Online* (2012) (<http://www.spiegel.de/international/world/the-nsa-uses-powerfultoolbox-in-effort-to-spy-on-global-networks-a940969.html> Accessed 06/06/2022

Tech Dirt, 'UK Spies Say They're Dropping Bulk Data Collection For Bulk Equipment Interference' *Tech Dirt* (2018) <https://www.techdirt.com/2018/12/12/uk-spies-say-theyre-dropping-bulk-data-collection-bulk-equipment-interference/> accessed 25/03/2022

The Intercept, 'Pull Through Steering Group Minutes' *The Intercept* (25/09/2015) <https://theintercept.com/document/2015/09/25/pull-steering-group-minutes/> accessed 06/06/2022

Thornhill J, 'Lunch with the FT: Pavel Durov' *Financial Times* (2015) https://www.ft.com/content/21c5c7f2-20b1-11e5-ab0f-6bb9974f25d0 accessed 06/06/2022

Turton W, 'What isn't Telegram saying about its connections to the Kremlin?' *The Outline* (2017) https://theoutline.com/post/2348/what-isn-t-telegram-saying-about-its-connections-to-the-kremlin accessed 06/06/2022

Books

Arai-Takahashi Y, 'The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR' (Antwerp: Intersentia, 2002)

Ashworth A and Redmayne M, *The Criminal Process* (4th edn, OUP 2010)

Cayford M, Gulijk CV and Gelder PHAJMv, 'All swept up: An initial classification of NSA surveillance technology' in Nowakowski T and others (eds), *Safety and Reliability: Methodology and Applications* (CRC Press 2014)

Craig, P and De Búrca, G 'EU Law : Text, Cases, and Materials'. (OUP 2020)

De Vries K, ''Right to Respect for Private and Family Life'' in al VDe (ed), *Theory and Practice of the European Convention On Human Rights* (Intersentia 2018)
Elliot M and Thomas R, *Public Law* (4th edn, Oxford University Press 2020)
Endicott T, *Administrative law* (4th edn, OUP 2018)
Fura E and Klamberg M, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA ' in Casadevall J, Myjer E and O'Boyle M (eds), *"Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights"* (Wolf Legal Publishers 2012)
Gillespie A and Weare S, *The English Legal System* (OUP 2019)
Glover R, *Murphy on Evidence* (15th edn, OUP 2017)
Greenwald G, *No place to hide: Edward Snowden, the NSA, and the US surveillance state* (Macmillan 2014)
Harris DJ and others, *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights* (Oxford University Press 2014)
Hawkins K, *Law as Last Resort: Prosecution Decision-Making in a Regulatory Agency* (OUP 2003)
Innes, J, *Privacy, Intimacy, and Isolation* (Oxford: Oxford University Press, 1992)
Karin De Vries, 'Right to Respect for Private and Family Life' in Dijk Pv and others (eds), *Theory and Practice of the European Convention on Human Rights* (5th edn, Intersentia 2018)
Leggatt A, *Tribunals for Users, One System, One Service* (HMSO 2001)
Michelle Madejski, Johnson ML and Bellovin SM, *The failure of online social network privacy settings* (Columbia Academic Commons, 2011)
Murphy CC, 'State Surveillance and Social Democracy' in Bogg A, Rowbottom J and Young AL (eds), *The Constitution of Social Democracy* (1 edn, Hart Publishing 2020)
Ruiz B, *Privacy in Telecommunications. A European and an American Approach* (Kluwer Law International 1997)
Stalla-Bourdillon S, Papadaki E and Chown T, 'Metadata, traffic data, communications data, service use information… What is the difference? Does the difference matter? An interdisciplinary view from the UK.' in Serge Gutwirth RL, Paul De Hert (ed), *Data Protection on the Move* (Springer 2016)
Stanton J and Prescott C, *Public Law* (2 edn, OUP 2020)
Thibaut JW and Walker L, *Procedural Justice: A Psychological Analysis.* (Erlbaum 1975)
Tyler RT and Yuen HJ, *Trust in the Law: Encouraging Public Cooperation with the Police and Courts.* (Russell-Sage Foundation 2002)

Yourow HC, *The margin of appreciation doctrine in the dynamics of European human rights jurisprudence* (Martinus Nijhoff Publishers 1996)

Websites

IPCO, 'Carrying out an inspection' (ipco.org.uk) <//www.ipco.org.uk/what-we-do/inspections/carrying-out-an-inspection/> accessed 29/09/2023

IPCO, 'Carrying out an inspection - bulk powers' (ipco.org.uk) https://www.ipco.org.uk/what-we-do/inspections/carrying-out-an-inspection/bulk-powers/ accessed 29/09/2023.

IPCO, 'Inspection Statistics' (ipco.org.uk) https://www.ipco.org.uk/what-we-do/inspections/inspection-statistics/ accessed 29/09/2023

IPCO, 'Selecting material for inspection' (ipco.org.uk) https://www.ipco.org.uk/what-we-do/inspections/selecting-material-for-inspection/ accessed 29/09/2023.

Investigatory Powers Tribunal, 'Closed and Open Procedure' (<https://www.ipt-uk.com/content.asp?id=13> accessed 07/06/2022

Investigatory Powers Tribunal, 'Frequently Asked Questions' (<https://www.ipt-uk.com/content.asp?id=24> accessed 07/06/2022

Investigatory Powers Tribunal, 'General Overview and Background' (<https://www.ipt-uk.com/content.asp?id=10 > accessed 07/06/2022

Milanovic M, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa' (*EJIL:Talk!*, 2021) <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> accessed 08/06/2022

Ni Loideain N, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment' (*Information Law and Policy Centre*, 2021) <https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/> accessed 08/06/2022